THE UNIVERSITY OF TEXAS AT AUSTIN

RECOMMENDATION FOR CHANGE IN ACADEMIC RANK/STATUS

Name: Tiwari, Mohit EID: mt28295 Present Rank: Assistant Professor

Years of Academic Service ***(Include AY 2018-19 in each count)***:

At UT Austin since: 9/1/2013 (month/day/year) Total Years at UT Austin: 6

In Present Rank since: 9/1/2013 (month/day/year) Total Years in Present Rank: 6

Tenure-track only:
Number of Years in Probationary Status: 6

Additional information: N/A

Primary Department: Electrical and Computer Engineering

College/School: Engineering, Cockrell School of

Joint Department: N/A

College/School: N/A

Other Department(s): N/A

Recommendation actions[1]:

By Budget Council/Executive Committee: Promote

Vote[2] for promotion 32; Against 0; Abstain 3; Absent 0; Ineligible to vote 2

By Department Chair: Promote

By College/School Advisory Committee: Promote

Vote[2] for promotion 7; Against 0; Abstain 0; Absent 0; Ineligible to vote 0

By Dean: Promote

Administrative Action: Promote to Associate Professor

Date Action Effective: September 1, 2019
(To be submitted to the Board of Regents as part of the annual budget.)

By: Date: February 15, 2019
For the President

[1] See "Chart of Recommended Actions" for eligible recommended actions applicable to specific conditions and administrative levels.

[2] Record all votes for and against promotion, abstentions by eligible voting members, and the number of absent eligible voting members. The number of committee members ineligible to vote should also be recorded. Enter zero where it would otherwise be blank.

EVPP/4.15

EXHIBIT
P's 147

The University of Texas at Austin
Cockrell School of Engineering

Dean's Assessment
Mohit Tiwari
Department of Electrical and Computer Engineering
Cockrell School of Engineering

Dr. Mohit Tiwari received his BTech in computer science and engineering in 2005 from the Indian Institute of Technology, Guwahati, and his MS and PhD in computer science from the University of California, Santa Barbara in 2010 and 2011, respectively. He was a post-doc at the University of California, Berkeley for two years before joining the Department of Electrical and Computer Engineering (ECE) as an assistant professor in September 2013. If promoted to associate professor in September 2019, he will have accumulated six years of probationary service.

Dr. Tiwari's research focuses on developing secure computer systems. The proliferation of computer systems, including social and cloud computing, has exacerbated security vulnerabilities. Traditional techniques of patching vulnerabilities as they are identified is no longer a sustainable approach to building secure computer systems that are needed for the healthcare, election, and mobile computing systems of the future. Dr. Tiwari has made important advances toward developing the hardware and software systems necessary to protect data. Important developments include architectural mechanisms that enable information-leak-free hardware enclaves, containerized data for web services, and anomaly-detection mechanisms. His work is directly related to one of the Cockrell School's four priority research areas: advancing intelligent systems and man-machine symbiosis.

Ten external letters were submitted as part of the promotion dossier, with six letter writers selected by the budget council. Nine letter writers are current or previous faculty members at peer universities in the US, and one is a principal research scientist at Visa Research.

Several connections exist between the letter writers and Dr. Tiwari, but I consider all of them to be arm's length reviewers:

- John Kubiatowicz (UC Berkeley) is technically not arm's length, as he is a co-author on a 2013 conference paper. As explained in the dossier, Dr. Tiwari was a post-doc at Berkeley when the research was conducted and Dr. Kubiatowicz was the co-advisor of one of the graduate students with whom Dr. Tiwari collaborated directly. However, Dr. Tiwari did not collaborate directly with Dr. Kubiatowicz.
- In his letter, Onur Mutlu (ETH Zürich and Carnegie Mellon) refers to a 2016 invited paper that summarized the topics presented during a conference session that he co-authored with Dr. Tiwari. This paper was a compilation of information presented by others and represents an editorial, rather than technical, collaboration.
- David Brooks (Harvard), Scott Mahlke (Michigan), Moinuddin Qureshi (Georgia Tech), and Dr. Tiwari are associated with C-FAR (Center for Future Architectures Research) at the University of Michigan. The center engages faculty at many universities (Michigan, Columbia, Duke, Georgia Tech, Harvard, Illinois, MIT, Princeton, Stanford, UC-Berkeley, UCLA, UC-San Diego, UT, Virginia, and Washington), and it does not appear that Dr. Tiwari has collaborated directly with any of the letter writers.

Teaching

While in rank, Dr. Tiwari taught one required undergraduate course and one graduate elective. He also organized a Freshman Research Initiative stream through the College of Natural Sciences, and served as a mentor. The CIS data from the FRI courses will not be addressed, because Dr. Tiwari was not directly responsible for teaching the courses.

Dr. Tiwari's instructor ratings have oscillated between 3.5 and 4.6 in the undergraduate course. In his teaching statement, Dr. Tiwari addressed the challenges he has faced in teaching the embedded systems course and the changes that he has made to improve the student satisfaction. He solicits feedback from the students throughout the semester, and appears to be receptive to their suggestions. His most challenging semester (Spring 2017) also corresponded to the largest number of students (78) in the class. He seems to have addressed the students' primary concerns, as his average instructor rating was much higher in Spring 2018.

Dr. Tiwari's teaching at the graduate level has been consistently strong.

Research

Dr. Tiwari has established a very strong, externally funded research program at UT. Key metrics include:

- 12 peer-reviewed proceedings at highly selective conferences in rank (22 total).[1] He published 8 conference papers with his students/post-docs at UT.
- 2 archival journal publications in rank (6 total). He published one journal paper with his students/post-docs at UT.
- He has published papers in highly selective conferences related to computer architecture and computer security, including International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), ACM Conference on Computer and Communications Security (CCS), IEEE International Symposium on Hardware Oriented Security and Trust (HOST), International Symposium on High Performance Computer Architecture (HPCA), International Symposium on Computer Architecture (ISCA), International Symposium on Microarchitecture (MICRO), and USENIX Security Symposium.
- An h-index of 19 (Google Scholar) and 1,271 citations.[2]

While in rank, Dr. Tiwari has secured 15 research grants/gifts totaling more than $5 million in external funding (his share is $3.5 million) from a wide variety of sources including three federal agencies[3] and industry. He is the PI on 14 of the grants. Three of his current grants extend beyond the end of the 2018-19 academic year, including two from NSF and one from DARPA.

The letters from the external reviewers were positive and addressed the impact of Dr. Tiwari's work and his reputation as an emerging leader. One reviewer made comments that can be considered to be critical, but he qualified his observation and recommended promotion:

[1] Refereed conference papers in highly selective conferences are the primary mechanism for disseminating research results in the fields of computer architecture and cyber security.

[2] Dr. Tiwari's most highly cited paper has 165 citations and is based on work completed during his graduate studies at UC-Santa Barbara. His most highly cited paper published in rank at UT has 78 citations.

[3] Defense Advanced Research Projects Agency (DARPA), National Science Foundation (NSF), and National Security Agency (NSA)

- John Kubiatowicz (Electrical Engineering and Computer Science, UC Berkeley) expressed some concerns about Dr. Tiwari's publication record, "his last 5 years have been fairly productive ... Mohit's paper count may be a bit lower than others in a similar position, but I'd say that it is more than sufficient."

Advising and Student Mentoring
Dr. Tiwari graduated one PhD student and three MS students. He co-mentored one postdoctoral fellow. He is currently advising seven PhD students (one co-supervised) and one MS student. He has also integrated undergraduate students into his research team with three to five students participating each year.

University Service
Dr. Tiwari's service to the university has primarily been related to faculty recruiting and graduate student recruiting. He has also been actively engaged in curriculum reform/development within ECE.

Professional Service
Dr. Tiwari is a member of several professional societies and actively serves on the program committees for top conferences in computer architecture and cybersecurity. He also serves as an associate editor for the *ACM Transactions of Code Optimization*.[4]

He contributes to the central Texas community by serving as a cybersecurity advisor for startups and Dell Children's Hospital.

Other Evidence of Merit or Recognition
Dr. Tiwari received a CAREER award from NSF in 2015 and he has received faculty research awards from Google (2014) and Qualcomm (2017). Several of his papers have been recognized with best paper awards.

Overall Assessment
Dr. Tiwari has established an outstanding reputation in computer architecture and cyber security. He has been extremely successful in securing external funding to sustain his research efforts. His teaching record is solid, and he is mentoring a large research group. He has provided excellent service to UT and professional communities within his field.

Overall, I believe that Dr. Tiwari's performance meets expectations in the area of teaching and exceeds expectations in the areas of research and service. Accordingly, I am pleased to provide my strong recommendation that Dr. Tiwari be promoted to associate professor with tenure.

Sharon L. Wood, Dean
10 November 2018

[4] The editorial board for ACM TACO includes 22 associate editors from around the world.

ELECTRICAL AND COMPUTER ENGINEERING DEPARTMENT
Cockrell School of Engineering

2501 Speedway · EER Building · Austin, Texas 78712-0240 (512) 471-6179 Fax (512) 471-3652
http://www.ece.utexas.edu

September 25, 2018

Chair's letter in support of the promotion of Prof. Mohit Tiwari to the rank of associate professor with tenure

Prof. Tiwari joined the Department of Electrical and Computer Engineering in August 2013. If promoted to associate professor in September of 2019, he will have served as an assistant professor at the University of Texas at Austin for six years.

Mohit is a recognized innovative researcher in secure and trustworthy computer systems. The Budget Council recognized his strong accomplishments and potential and determined that he meets all expectations for promotion at the premier departments of Electrical and Computer Engineering in the nation by a vote of 32 YES, 0 NO and 3 ABSTAIN and 2 INELIGIBLE TO VOTE. The ineligible votes are Prof. Mark Smith's and mine. Our associate professors voted 10 YES, 0 NO and 0 ABSTAIN in support of promotion. My colleagues expressed considerable support for Mohit during the promotion discussion and in the anonymous comments submitted with the vote. I therefore assume that the abstentions are due to a lack of familiarity with his case.

Third Year Review

The committee that conducted the third-year review of Prof. Tiwari concluded that he had "a solid record in research, teaching, and service," there were "no concerns regarding his performance and productivity" and felt "that Prof. Tiwari exceeds expectations." I concurred with the committee. The committee was particularly impressed by his teaching skills and especially by his efforts to create a new Freshman Research Initiative course on security in collaboration with the Department of Computer Science in the College of Natural Sciences. The committee was also very impressed by his publication record and ability to raise funding for his research.

Teaching Load of Assistant Professors

The normal teaching load for a tenure-track assistant professor is two courses per academic year plus supervision of a senior design team for two semesters. One of the courses must be an undergraduate course. This requirement is waived only under exceptional circumstances if the department has unmet needs at the graduate level. Faculty in the department are routinely given modified instructional duties upon the birth of a child.

Teaching

Mohit is a dedicated instructor. He regularly teaches our freshman required introduction to embedded systems EE319K. His instructor score in that course started low at 3.8 and rose to 4.6 last semester, with a drop during the spring 2017 semester to 3.5. I attribute the low score in 2017 to several factors, including the fact that Mohit missed the first few weeks of class after encountering long delays in getting a US visa while visiting India over the winter break and using online as opposed to paper course surveys and not requesting students to fill the form . His graduate teaching instructor scores are all above 4.0.

Mohit does an excellent job of helping freshman students understand that the field of embedded computing is rapidly changing. He regularly manages to convince students that they need to master the fundamentals presented in the class and apply them creatively to remain relevant. In his unrelenting quest to form future innovators, he encourages students to get involved in research opportunities at UT and helps them secure internships in marquee companies. In two of the four years that he has taught the course, a team from his section won the best game competition across all EE319 K sections.

As mentioned above, Mohit also designed a freshman Research Initiative course on security in collaboration with the Department of Computer Science. He took the initiative to create the stream and was involved in delivering it on an overload basis. He selected and made assignments for the three semester courses in the stream, chose papers to be read and trained the Research Educator who delivered the lectures. Mohit attended the lectures, occasionally interjecting in discussions and providing guidance to the Research Educator. The CIS scores by the two or three ECE students who were allowed to take the stream do not reflect Mohit's teaching ability—rather they reflect the confusion of the students did not understand why they are were required to complete CIS forms about Mohit when he was not the in-class lecturer.

In yet another example of Mohit's teaching skills and the high esteem in which his colleagues hold him, one of our more senior professors who struggled in teaching went to Mohit seeking help. Mohit quickly realized that the problems that our colleague faced stemmed from the way he created questions on his assignments and exams. It is interesting to note that the feedback provided by Mohit was the only effective feedback that our colleague received from faculty members within and outside the department who had observed him in the classroom and looked at his assignments. With Mohit's advice, our colleague was able to substantially increase his instructor scores in undergraduate courses.

Mohit also took the initiative to create a truly unique course on security with our information security office. A heavy reliance on manipulation and examination of actual data in real-time collected by our information security office sets this course apart from other security courses taught across the nation. It provides students a solid grounding in theory and practice.

Mohit is also playing a leadership role in creating an interdisciplinary portfolio of security courses taught by Electrical and Computer Engineering and Computer Science faculty members.

The student comments clearly indicate that Mohit cares about the students, is very passionate about what he teaches and is approachable. Some EE 319 K students complain about inadequate coverage of material from the laboratories and the course being not well structured. EE 319 K is team taught and these shortcomings reflect the choices made by the team. This of course does not absolve the individual instructors of using the student feedback to improve the course delivery. Mohit's peers commend him for his engaging lecturing style and, like the students, have encouraged him to improve his handwriting.

Mohit graduated one PhD student in rank. The student joined a mobile-phone and home-automation startup, Essential. His Master's advisees joined Apple, Nvidia and ARM.

Research

Recurring high visibility data breaches underscore the importance of Mohit's area of research in secure and trustworthy computer systems. Many of these breaches caught experts by surprise as no one foresaw the vulnerability of several techniques that researchers had developed, and designers deployed, to improve the performance of computer architectures. For example, Intel and processor manufacturers found that features built into their chips over the last two decades have introduced subtle vulnerabilities that subvert all software security mechanisms. Mohit's work is undoubtedly one of the most successful and highly visible efforts to address the vulnerability in modern computer architectures. He was one of the pioneers of a data-centric approach to security that relies on securing all aspects of memory and computational units design, access and control.

In the data-centric paradigm promoted by Mohit, users own their data and applications run inside a user-controlled "secure enclave." A secure enclave is a section of a computational system that is segregated from the rest of the system. A secure enclave may use a separate processor, boot separately from the rest of the system and run a microkernel that is not directly accessible by the general operating system or any programs running on the system. It can run programs without generating clues that an attacker can observe to guess what programs were running and reconstruct the data that was processed. The paradigm proposed by Mohit exploits several hardware-software primitives that he proposed in rank: i) containers that can enclose untrusted applications inside and run on untrusted cloud providers on the outside; ii) a programming model that enables developers to write feature-rich applications that can be data-containerized, and iii) a machine learning system that identifies new attacks as computational anomalies on each device and tracks these anomalies as they propagate across a network.

Mohit's work on secure enclaves has garnered extensive visibility and is mentioned in all his reference letters. Previous research has shown that information about data or programs can be inferred by monitoring power consumption and electromagnetic admissions, and most importantly, the "side-channels" that are embedded within the operating system or hardware architecture and are conventionally used to enhance performance by monitoring the execution of a program. In a series of ground breaking and award-winning papers, Mohit showed how one can use properly designed static control and data flow to eliminate any information leakage. His work establishes a formal design process with performance guarantees to construct information-leak-free enclaves. This is to be contrasted with the "band-aid" response to specific attacks and other ad hoc security methods that prevail today. Each iteration of the systems proposed by Mohit is moving us closer to practical implementation of the concept. Mohit's work in this area is comprehensive—covering instruction sets, compilers and programming annotations. Four of his papers in this area from 2014 to this year won distinguished recognitions including a top-10 applied security paper, a top-pick architecture paper, a best paper and a best paper nomination. Prof. Kubiatowicz (UC Berkeley) describes the work as "fascinating." Prof. Devadas (MIT) characterizes some of the papers that Mohit wrote in this area as "groundbreaking" and notes that the work motivated his own research. Prof. Mahlke (Michigan) states that he is "impressed by this work because of both the difficulty of the problem sold as well as the rigor and completeness of the solution."

His more recent work on programming large-scale web-services on data-container systems has also achieved widespread recognition. As several high-profile data breaches (Target, Equifax, etc.) have recently shown, data can be exposed by breaching large-scale web-services infrastructures. Mohit's brilliant insight was to design access control rules that break any database into smaller sections and restrict any instance of a given application to a single data section at any given time. This strategy effectively eliminates the ability of any malicious application to leak an entire database to an attacker. The approach has been dubbed DATS by Mohit. Prof. Kruegel (UCSB) describes the work as an "interesting mix of hardware-capability-enhanced containers and two new primitives" and notes that "Mohit's evaluation, where he applies the new techniques to real world programs such as get Gitlab, convincingly addresses these concerns and shows that the approach has cleared world potential." Prof. Kubiatowicz states that it "seems like a very interesting future direction to help prevent data breaches" an notes that "this work is already being adopted in industry – a clear sign that it addresses and industry-visible need." Indeed, several cloud-providers such as CenturyLink and Rackspace are piloting the approach to prevent by Equifax-like breaches. Mohit is also collaborating with Visa Research to transition this work into financial services.

To complement his work on secure enclaves and web-services based on data-container systems, Mohit introduced anomaly detectors that can pre-emptively detect a wide class of attacks. This work is based on another clever observation: Hypervisors and operating systems are not designed to monitor microarchitecture usage. Hence, malware and other attacks can hide hardware level computations from operating systems. To defeat malware and attacks, Mohit proceeded to expose and analyze the instruction-set of running applications and micro-architecture behavior. By modeling hardware structures as communication channels, he converts the detection of malicious behavior to the well-understood problem of detecting interference in communication channels. Prof. Mutlu (ETH) notes that "first such treatment that I know of" This work has been showcased at several meetings sponsored or organized by NSF, NIST, NSA, and several universities and companies. The work was also transitioned to Qualcomm. I attribute the two Qualcomm faculty awards that Mohit received last year and this month to this work. I note that the Qualcomm Faculty Award is based on internal Qualcomm assessment of academic research with no external input, application or nomination.

Prof. Tiwari is very well funded by highly competitive peer-reviewed grants and industry. I expect his funding to increase even further because of his new discoveries and increased awareness of his inventions.

Our department has adopted the practice of comparing each colleague with his or her most prominent peers at the first-tier departments in Electrical and Computer Engineering, such as MIT, Stanford, the University of California Berkeley, the University of Illinois Urbana-Champaign (UIUC), Georgia Tech, Caltech and Princeton. I selected Associate Profs. Edward Suh (Cornell), Daniel Sanchez (MIT) and Simha Sethumadhavan (Columbia) to be the peer comparison group for Mohit. Suh and Sethumadhavan were promoted to the rank of associate professor with tenure in 2013, while Sanchez was promoted to associate professor in 2017. Mohit compares very favorably to all three associate professors. While Suh has a current citation count and h-index that are higher than all three other professors, including Mohit, Mohit has more papers in the top-ranked conferences than any of the other three professors except for Sanchez, and has the largest number of award-winning papers. Industry and the research community have recognized the potential impact of his work. All reviewers recognized his accomplishments, the impact of his work and promise relative to his peers. Their recommendations are best summarized by the following statements by Prof. Devadas "In the field of secure architecture, in my opinion, Mohit has done the best work of anyone in his age group (or pre-tenure) over the past several years… Mohit's work stands out because he builds the "right" kind of systems, where at least the specification of the system can be proven to have strong security guarantees that are convincing to system security and cryptography researchers alike" and Myers (Cornell) "His work is consistently creative, and he is connecting the security and hardware communities in ways that are important for the intellectual health of these communities and that show he is a master of both domains …I would say that Dr. Tiwari is probably the top faculty member of his approximate academic age at the increasingly important hardware/security boundary."

	PhD	Promoted	Publications in top conferences at promotion	H Index	Citations
Edward Suh (Cornell)	2005	2013	6	27	6650
Simha Sethumadhavan (Columbia)	2007	2013	7	21	2221
Daniel Sanchez (MIT)	2012	2017	15	16	1532
Mohit Tiwari (UT Austin)	2011		12	17	1037

Service

Mohit has provided excellent service to the department. I will note in particular that Mohit played a key role several times on our faculty recruiting committees. These committees are labor intensive as they require proactive outreach and recruiting efforts across the multiple areas spanned by the department. He has played key leadership roles in promoting several large partnerships with companies. Despite being the most junior faculty member in cybersecurity at UT, he has and continues to play a leadership role in the joint computer science and electrical and computer engineering cybersecurity initiative that aims at attracting additional star researchers to our faculty and establish a comprehensive curriculum in cybersecurity.

Summary

Mohit is a dedicated teacher and a highly creative researcher credited with inventing several new breakthroughs in cybersecurity despite his young age. One of my colleagues summarizes the case by stating that "This is a very strong case. We are fortunate to have Mohit as a colleague." I strongly endorse his promotion to associate professor with tenure.

Sincerely,

A. Tewfik

Prof. Ahmed H. Tewfik
Cockrell Family Regents Chair in Engineering
Chairman, Department of Electrical and Computer Engineering

Third Year Review 2015
Mohit Tiwari

Prof. Tiwari graduated with a Bachelor of Technology in 2005 from the Indian Institute of Technology in Guwahati. He received his M.S. and Ph.D. in Computer Science from the University of California at Santa Barbara in 2010 and 2011, respectively. From 2011 to 2013 he was a post-doc at the University of California at Berkeley. He joined our faculty as an Assistant Professor in 2013.

Teaching

Over the last 2.5 years, Prof. Tiwari has taught two graduate and two undergraduate courses. At the graduate level, he twice taught the new course he introduced on Security at the Hardware-Software Interface. His instructor ratings over the two offerings have been very high (4.0-4.5), which is near the average for the graduate courses in Electrical and Computer Engineering. The student comments for these classes are very positive. At the undergraduate level, he taught the Introduction to Embedded Systems and his instructor rating was 3.8, slightly below the average for this course (4.0). The students' comments are positive, praising Prof. Tiwari's enthusiasm and interest. Considering that this was his first time teaching the course, the rating does not cause a concern. We expect Prof. Tiwari to continue improving his lecture-hall skills and become an outstanding lecturer over a short period of time.

Prof. Tiwari's interest in undergraduate teaching is further evidenced by his efforts to create a new Freshman Research Initiative course on security in collaboration with the Computer Science Department of the College of Natural Sciences. Through this activity, Mohit has contributed to making UT's Freshman Research Program the Nation's largest such program.

Research

Prof. Tiwari's research focuses on computer architecture and the design of secure systems. His interests in this area are unusually wide, ranging from tracking the flow of information in the computing systems to determine potential vulnerabilities to side-channel attack analysis to privacy-preserving algorithms. Prof. Tiwari is technically outstanding and brings to his research a combination of theoretical rigor and a passion for solving practically-critical problems. In the short period of time, he has already established himself as one of the leaders of the systems security area. There is plentiful evidence in support of that assessment. He has received multiple awards including, the NSF CAREER Award in 2015, Google faculty award, NYU-Poly Top 10 applied security paper of the year, two Best Paper Awards at leading conferences (ASPLOS, PACT), and the IEEE Micro Top Picks mention. He has also been invited to join a multi-university computer architecture research center.

Since joining UT Austin, Prof. Tiwari has been very productive. He has produced 8 journal or highly selective conference publications. In the area of computer architecture and security, conference publications are considered to be the primary publication vehicles. Prof. Tiwari's papers have been published in the leading conferences. He has secured over $1.77M in research grants in the last 2.5 years (his share), from diverse sources including the National Science Foundation, Department of Defense, a DARPA-funded multi-university research center, and various companies (Google, Samsung, Huwaei). He has several proposals that have been submitted, mostly to NSF, and are in the process of being evaluated.

Advising and Student Mentoring

In the 2013-2014 academic year Prof. Tiwari started supervising two PhD students. During his second academic year his group rose to six PhD students. He anticipates in the 2014-2015 academic year that five of these students will be supported by grants and one will be supported by a TA or fellowship. He has not graduated any Ph.D. students yet. The committee feels since he is currently supervising six Ph.D. students, he is well positioned to have a strong tenure promotion case.

Professor Tiwari supervised a senior lab group in security on smart automobiles. He has recruited 8 undergraduate students (outside of the FRI class and the senior design project) to conduct research in mobile malware analysis and cloud security projects

University Service

Prof. Tiwari was an active leader in the Freshman Research Initiative (FRI). This is a three semester sequence for a cohort of 17 students participating in open-ended research.

During the 2014-2015 year, Professor Tiwari was on the ECE Faculty recruitment committee, focusing on security and computer architecture/systems. He was on the Computer Architecture and Embedded Processor graduate admissions committee. He helped host the graduate student visit day.

Professional Service

Prof. Tiwari served on the Program committees for top architecture and security conferences: ISCA (2014, 2015), HPCA (2015), Oakland Security and Privacy (2015). He was on the external review committee for ASPLOS (2015). He was also on the PC for CGO (2014, 2015), ISPASS (2014), and HASP (2014). He served on an NSF Panel for Secure and Trustworthy Cyberspace.

Overall Assessment

Prof. Tiwari has a solid record in research, teaching, and service. There are no concerns regarding his performance and productivity. The Committee feels that Prof. Tiwari exceeds expectations.

Electrical and Computer Engineering Revised September 17, 2018

THE UNIVERSITY OF TEXAS AT AUSTIN
Cockrell School of Engineering
Standard Resume

FULL NAME: Mohit Tiwari **TITLE:** Assistant Professor

DEPARTMENT: Electrical and Computer Engineering

EDUCATION:

University of California, Santa Barbara	Computer Science	Ph.D.	July 2011
University of California, Santa Barbara	Computer Science	M.S.	July 2010
Indian Institute of Technology, Guwahati	Computer Science and Engineering	B. Tech.	June 2005

PROFESSIONAL REGISTRATION:

CURRENT AND PREVIOUS ACADEMIC POSITIONS:

University of Texas at Austin	Assistant Professor	Aug 2013 –
University of California, Berkeley	NSF Computing Innovation Post-doctoral Fellowship	Aug 2011 – July 2013

OTHER PROFESSIONAL EXPERIENCE:

University of California, Santa Barbara	Graduate Research Assistant	June 2006 – July 2011
Naval Postgraduate School, Monterey	Research Visitor	Aug 2008 – Sept 2008
NEC Laboratories, Princeton, NJ	Research Intern	June 2007- Aug 2007
University of California, Santa Barbara	Teaching Assistant	Sept 2005- May 2006

CONSULTING:

Intel, Hillsboro, OR	April 2018 –
Privasera Inc, Austin, TX	June 2015 –

HONORS AND AWARDS:

2018 – Best Paper Award Runner-up, International Symposium on Hardware-Oriented Security and Trust (HOST)

2018 – Plenary Speaker, National Science Foundation workshop on Side- and Covert-Channels Security, Washington D.C.

2017 – Qualcomm Faculty Award, for technology transfer of MICRO'16 paper on hardware-based malware detection

2017 – AMD Chair (UT ECE Department)

2017 – Invited to teach at the International Summer School on Advanced Computer Architecture and Compilation for High-Performance and Embedded Systems (ACACES), Fiuggi, Italy
2016 – Keynote speaker, Workshop on Computer-Aided Design and Implementation for Cryptography and Security (CADICS) at the International Conference on Computer-Aided Design (ICCAD)
2015 – Best Paper Award, International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)
2015 – National Science Foundation CAREER award
2015 – IEEE Micro Top Picks of the Year in Computer Architecture, Honorable Mention
2014 – Google Faculty Research Award
2013 – NYU-CSAW Best Applied Security Paper of the Year, top-10.

2011 – 2013 National Science Foundation Computing Innovation Postdoctoral Fellowship
2011 – Outstanding Dissertation Award, Department of Computer Science, UC Santa Barbara
2010 – IEEE Micro Top Picks of the Year in Computer Architecture
2009 – Best Paper Award, International Conference on Parallel Architectures and Compilation Techniques (PACT)
2006 – Outstanding Teaching Assistant, Dept. of Computer Science & Engineering, UC Santa Barbara

MEMBERSHIPS IN PROFESSIONAL AND HONORARY SOCIETIES:

- Institute of Electrical and Electronics Engineers (IEEE)
- Association of Computing Machinery (ACM)

UNIVERSITY COMMITTEE ASSIGNMENTS:

Departmental-	ECE Junior Faculty Search Committee	2014-'15, 2017-'18
	ECE Senior Faculty Search Committee	2015-'16, 2016-'17
	ECE Graduate Admissions for ACSES/SES	2013—
	ECE Curriculum Reforms Committee	2016—

PROFESSIONAL SOCIETY AND MAJOR GOVERNMENTAL COMMITTEES:

- Program committee member for architecture-systems conferences
  - International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS) – 2015, 2018, 2019
  - International Symposium on Computer Architecture (ISCA) – 2014, 2015
  - International Symposium on Microarchitecture (MICRO) – 2015, 2018
  - International Symposium on High Performance Computer Architecture (HPCA) – 2015, 2017
  - International Conference on Code Generation and Optimization (CGO) – 2015
  - International Conference on Performance Analysis of Systems and Software (ISPASS) – 2015
- Program committee member for computer security conferences
  - International Conference on Computer and Communication Security (CCS) – 2015, 2016, 2017, 2018
  - International Symposium on Security and Privacy (S&P "Oakland") – 2015, 2016

  - International Symposium on Hardware Oriented Security and Trust (HOST) – 2016, 2017, 2018
- Associate Editor for ACM Transactions on Architecture and Code Optimization (TACO) – 2017 – present
- NSF proposal panel reviewer for the Secure and Trustworthy Computing (SaTC) program – 2014, 2015, 2016, 2017, 2018
- Guest Editor, IEEE Micro Magazine (Special Issue on Security) – Sept-Oct 2016
- Paper Reviewer for IEEE/ACM Conferences and Journals – ISCA, MICRO, ASPLOS, HPCA, CGO, ISPASS, S&P, CCS, PLDI, CAL, TACO, TOCS.

COMMUNITY ACTIVITIES:

- Setting up a cybersecurity operations laboratory with the CISO of UT Austin (Cam Beasley) to enable research using UT's network as an experimental test-bed – Spring 2018

- Contributing to starting a cybersecurity curriculum for ECE students, with undergraduate and graduate systems security courses as well as a course on cybersecurity operations that uses live data from UT's network.

- Taught a Freshman Research Initiative (FRI) stream on cybersecurity, in collaboration with Dr. Calvin Lin (CS department) – 2015, 2016.

PUBLICATIONS: ((in rank publications shown in bold)
Google Scholar link: https://scholar.google.com/citations?user=FukOricAAAAJ&hl=en

Mohit Tiwari's students/advisees are *italicized.* The students in this list include

- Graduate student PhD advisees (funded as GRAs): Mikhail Kazdagli, Casen Hunger, Austin Harris, Ashay Rane
- Undergraduate advisees (funded as undergraduate RAs): Manuel Philipose, Youssef Tobah
- Visiting graduate-student researchers in my lab: Lluis Vilanova (funded by a fellowship to work in my lab)
- Post-doctoral scholars (who worked with me, and funded by grants I am the PI on): Aydin Aysu
- Graduate students (unfunded, who worked on project in my graduate class): Matthew Halpern (advisor: Vijay Janapa Reddi), Hardik Jain (advisor: Sriram Vishwanath)

A. Refereed Archival Journal Publications

1. Mohit Tiwari, Xun Li, Hassan Wassel, Bita Mazloom, Shashidhar Mysore, Frederic Chong, and Timothy Sherwood, "Gate-Level Information-Flow Tracking for Secure Architectures," *IEEE Micro Top Picks from Computer Architecture Conferences*, January-February 2010. https://doi.org/10.1109/MM.2010.17

2. Wei Hu, Jason Oberg, Ali Irturk, Mohit Tiwari, Timothy Sherwood, and Ryan Kastner, "Theoretical Fundamentals of Gate Level Information Flow Tracking", IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), August 2011. https://doi.org/10.1109/TCAD.2011.2120970

3. Hassan Wassel, Daoxin Dai, Luke Theogarajan, Jennifer Dionne, Mohit Tiwari, Jonathan Valamehr, Frederic Chong, and Timothy Sherwood, "Opportunities and Challenges of Using Plasmonic Components in Nanophotonic Architectures," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems,* June 2012. https://doi.org/10.1109/JETCAS.2012.2193934

4. Wei Hu, Jason Oberg, Ali Irturk, Mohit Tiwari, Timothy Sherwood, Dejun Mu and Ryan Kastner, "On the Complexity of Generating Gate Level Information Flow Tracking Logic," *IEEE Transactions on Information Forensics and Security* (TIFS), June 2012. https://ieeexplore.ieee.org/document/6159079/

5. Bita Mazloom, Shashidhar Mysore, Mohit Tiwari, and Timothy Sherwood, "Dataflow Tomography: Information Flow Tracking for Understanding and Visualizing Full Systems," *ACM Transactions on Architecture and Code Optimization* (TACO) September 2012. https://doi.org/10.1145/2133382.2133385

6. **Wei Hu, Dejun Mu, Jason Oberg, Baolei Mao, Mohit Tiwari, Timothy Sherwood, Ryan Kastner, "Gate Level Information Flow Tracking for Security Lattices," *ACM Transactions on Design Automation of Electronic Systems* (TODAES), Volume 20, November 2014. https://doi.org/10.1145/2676548**

7. **Pavel Lifshits, Roni Forte , Yedid Hoshen, *Matthew Halpern, Manuel Philipose*, Mohit Tiwari, and Mark Silberstein, "Power to peep-all: Inference Attacks by Malicious Batteries on Mobile Devices", in Proceedings on Privacy Enhancing Technologies (PoPETs), July 2018.** https://www.petsymposium.org/2018/files/papers/issue4/popets-2018-0036.pdf

B. Refereed Conference Proceedings (in rank publications shown in bold)

1. Mohit Tiwari, Banit Agrawal, Shashidhar Mysore, Jonathan K Valamehr, and Timothy Sherwood, "A Small Cache of Large Ranges: Hardware Methods for Efficiently Searching, Storing, and Updating Big Dataflow Tags," *Proceedings of the International Symposium on Microarchitecture* (MICRO), November 2008. Lake Como, Italy. https://doi.org/10.1109/MICRO.2008.4771782

2. Mohit Tiwari, Hassan Wassel, Bita Mazloom, Shashidhar Mysore, Frederic Chong, and Timothy Sherwood, "Complete Information Flow Tracking from the Gates Up," *Proceedings of the 14th International Conference on Architectural Support for Programming Languages and Operating Systems* (ASPLOS), March 2009. Washington, DC. https://doi.org/10.1145/1508244.1508258

3. Mohit Tiwari, Shashidhar Mysore, Timothy Sherwood, "Quantifying the Potential for Program Analysis Peripherals," *Proceedings of the International Conference on Parallel Architecture and Compilation Techniques* (PACT), September 2009, Raleigh, NC (**Best Paper Award).** https://doi.org/10.1109/PACT.2009.38

4. Mohit Tiwari, Xun Li, Hassan M G Wassel, Frederic T Chong, Timothy Sherwood, "Execution Leases: A Hardware-Supported Mechanism for Enforcing Strong Non-Interference," *Proceedings of the International Symposium on Microarchitecture* (MICRO), December 2009, New York, NY. https://doi.org/10.1145/1669112.1669174

5. Jason Oberg, Wei Hu, Ali Irturk, Mohit Tiwari, Timothy Sherwood and Ryan Kastner, "Theoretical Analysis of Gate Level Information Flow Tracking," *Proceedings of the 47th Design Automation Conference* (DAC), June 2010, Anaheim, CA. https://doi.org/10.1145/1837274.1837337

6. Jonathan Valamehr, Mohit Tiwari, Timothy Sherwood, Ryan Kastner, Ted Huffmire, Cynthia Irvine, Timothy Levin, "Hardware Assistance for Trustworthy Systems through 3-D Integration," *Proceedings*

of the Annual Computer Security Applications Conference (ACSAC), December 2010, Orlando, FL. https://doi.org/10.1145/1920261.1920292

7. Xun Li, Mohit Tiwari, Jason Oberg, Vineeth Kashyap, Frederic T Chong, Timothy Sherwood, and Ben Hardekopf, "Caisson: A Hardware Description Language for Secure Information Flow," *Proceedings of the ACM Conference on Programming Language Design and Implementation* (PLDI), June 2011, San Jose, CA. https://doi.org/10.1145/1993316.1993512

8. Jason Oberg, Wei Hu, Ali Irturk, Mohit Tiwari, Timothy Sherwood, Ryan Kastner, "Information Flow Isolation in I2C and USB," *Proceedings of the 47th Design Automation Conference* (DAC), June 2011, San Diego, CA. https://doi.org/10.1145/2024724.2024782

9. Susmit Biswas, Mohit Tiwari, Luke Theogarajan, Timothy Sherwood, and Frederic T. Chong "Fighting Fire with Fire: Modeling the Data Center Scale Effects of Targeted Superlattice Thermal Management," *Proceedings of the International Symposium of Computer Architecture* (ISCA), June 2011, San Jose, CA. https://doi.org/10.1145/2024723.2000104

10. Mohit Tiwari, Jason Oberg, Xun Li, Jonathan K Valamehr, Timothy Levin, Ben Hardekopf, Ryan Kastner, Frederic T Chong, Timothy Sherwood, "Crafting a Usable Microkernel, Processor, and I/O System with Strict and Provable Information Flow Security," *Proceedings of the International Symposium of Computer Architecture* (ISCA), June 2011, San Jose, CA. http://doi.org/10.1145/2000064.2000087

11. **Martin Maas, Eric Love, Emil Stefanov, Mohit Tiwari, Elaine Shi, Krste Asanović, John Kubiatowicz, Dawn Song, "PHANTOM: Practical Oblivious Computation in a Secure Processor", *Proceedings of the ACM Conference on Computer and Communications Security* (CCS), November 2013, Berlin, Germany. (NYU-CSAW Best Applied Security Paper of the Year, top-10.) https://doi.org/10.1145/2508859.2516692**

12. **Xun Li, Vineeth Kashyap, Jason Oberg, Mohit Tiwari, Vasanth Rajarathinam, Ryan Kastner, Timothy Sherwood, Ben Hardekopf, and Frederic Chong, "Sapper: A Language for Hardware-Level Security Policy Enforcement," *Proceedings of the 14th International Conference on Architectural Support for Programming Languages and Operating Systems* (ASPLOS), March 2014, Salt Lake City, UT. (IEEE Micro Top Picks of the Year in Architecture, Honorable Mention.) https://doi.org/10.1145/2644865.2541947**

13. ***Casen Hunger, Mikhail Kazdagli,* Ankit Rawat, Alex Dimakis, Sriram Vishwanath, Mohit Tiwari, "Understanding Contention-driven Covert Channels and Using Them for Defense", *Proceedings of the International Symposium on High Performance Computer Architecture* (HPCA), February 2015, San Francisco, CA. https://doi.org/10.1109/HPCA.2015.7056069**

14. **Chang Liu, *Austin Harris,* Martin Maas, Michael Hicks, Mohit Tiwari, Elaine Shi, "GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation," *Proceedings of the 15th International Conference on Architectural Support for Programming Languages and Operating Systems* (ASPLOS), March 2015, Istanbul, Turkey. (Best Paper Award.) https://doi.org/10.1145/2694344.2694385**

15. **Ali Shafiee, Akhila Gundu, Manjunath Shevgoor, Rajeev Balasubramonian, Mohit Tiwari, "Avoiding Information Leakage in the Memory Controller with Fixed Service Policies," *Proceedings of the 48th***

International Symposium on Microarchitecture (MICRO), December 2015, Waikiki, HI. https://doi.org/10.1145/2830772.2830795

16. *Ashay Rane*, Calvin Lin, Mohit Tiwari, "Raccoon: Closing Digital Side-Channels through Obfuscated Execution," *Proceedings of the 24th USENIX Security Symposium*, August 2015, Washington, D.C. https://www.usenix.org/node/190909

17. *Ashay Rane*, Calvin Lin, Mohit Tiwari, "Secure, Precise, and Fast Floating-Point Operations on x86 Processors," *Proceedings of the 25th Usenix Security Symposium*, August 2016, Austin, TX. https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/rane

18. *Mikhail Kazdagli*, Vijay Janapa Reddi, Mohit Tiwari, "Quantifying and Improving the Efficiency of Hardware-based Mobile Malware Detectors," *Proceedings of the 49th International Symposium on Microarchitecture* (MICRO), October 2016, Taipei, Taiwan. (Transitioned to Qualcomm Malware Research team, led to Qualcomm Faculty Award 2017.) https://doi.org/10.1109/MICRO.2016.7783740

19. Ali Shafiee, Rajeev Balasubramonian, Mohit Tiwari, Feifei Li, "Secure DIMM: Moving ORAM Primitives Closer to Memory," *Proceedings of International Symposium on High Performance Computer Architecture* (HPCA), February 2018, Vienna, Austria. https://doi.org/10.1109/HPCA.2018.00044

20. *Aydin Aysu*, Michael Orshansky, Mohit Tiwari, "Binary Ring-LWE Hardware with Power Side-Channel Countermeasures," *Proceedings of Design Automation and Test in Europe* (DATE), March 2018, Dresden, Germany. https://doi.org/10.23919/DATE.2018.8342207

21. *Casen Hunger, Lluis Vilanova**, Charalampos Papamanthou, Yoav Etsion, Mohit Tiwari, "DATS: Data Containers for Web Applications," *Proceedings of Architectural Support for Programming Languages and Operating Systems* (ASPLOS), March 2018, Williamsburg, VA. https://doi.org/10.1145/3173162.3173213
**Lluis Vilanova worked on this paper as a visitor in my lab in Fall 2014.*

22. *Aydin Aysu, Youssef Tobah*, Mohit Tiwari, Andreas Gerstlauer, Michael Orshansky, "Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange Protocols," *Proceedings of IEEE Internation Symposium on Hardware Oriented Security and Trust* (HOST), May 2018, Washington DC, USA. (Best Paper Award, Runner-up.) http://spark.ece.utexas.edu/pubs/HOST-18-pqdpa.pdf

C. Other Major Publications (in rank publications shown in bold)
(Technical Workshop Proceedings, Non-technical/education-related documents.
Note: not all publications have DOI entries; please contact tiwari@austin.utexas.edu or visit http://spark.ece.utexas.edu to access the documents)

1. Ashish Sharma, Mohit Tiwari, Haitao Zheng, "Madmac: Building a Reconfigurable Radio Testbed using Commodity 802.11 Hardware," *IEEE Workshop on Networking Technologies for Software Defined Radio Networks*, September 2006, Reston, VA. https://doi.org/10.1109/SDR.2006.4286329

2. Xun Li, Mohit Tiwari, Ben Hardekopf, Timothy Sherwood, and Frederic Chong, "Secure Information Flow Analysis for Hardware Design: Using the Right Abstraction for the Job," *Proceedings of the Fifth ACM SIGPLAN Workshop on Programming Languages and Analysis for Security* (PLAS), June 2010.

3. Xun Li, Mohit Tiwari, Timothy Sherwood, Frederic Chong, "Function Flattening for Lease-Based, Information-Leak-Free Systems," *21st IEEE International Conference on Application-specific Systems, Architectures and Processors* (ASAP Poster), July 2010, Rennes, France.

4. Ted Huffmire, Timothy Levin, Michael Bilzor, Cynthia Irvine, Jonathan Valamehr, Mohit Tiwari, Timothy Sherwood, Ryan Kastner, "Hardware Trust Implications of 3-D Integration," *Workshop on Embedded Systems Security* (WESS) October 2010, Scottsdale, AZ.

5. Hassan Wassel, Mohit Tiwari, Jonathan K. Valamehr, Luke Theogarajan, Jennifer Dionne, Frederic T. Chong, Timothy Sherwood, "Towards Chip-Scale Plasmonic Interconnects," *Workshop on the Interaction between Nanophotonic Devices and Systems* (WINDS), December 2010. Atlanta, GA.

6. Wei Hu, Jason Oberg, Ali Irturk, Mohit Tiwari, Timothy Sherwood, Dejun Mu, Ryan Kastner, "An Improved Encoding Technique for Gate Level Information Flow Tracking," *International Workshop on Logic and Synthesis* (IWLS), June 2011.

7. Janet Kayfetz, Henning Schulzrinne, Timothy Sherwood, and Mohit Tiwari, "Your Desktop or Mine: Extending the Reach of Writing Instruction," *Ubiquitous Learning: An International Journal Volume 3, No 3.*, September 2011.

8. Mohit Tiwari, Prashanth Mohan, Andrew Osheroff, Hilfi Alkaff, Elaine Shi, Eric Love, Dawn Song, Krste Asanovic, "Context-centric Security," *Proceedings of the 7th USENIX Workshop on Hot Topics in Security* (HotSec), August 2012, Bellevue, WA. https://www.usenix.org/conference/hotsec12/workshop-program/presentation/tiwari

9. **Martin Maas, Eric Love, Emil Stefanov, Mohit Tiwari, Elaine Shi, Krste Asanovic, John Kubiatowicz, Dawn Song, "A High-Performance Oblivious RAM Controller on the Convey HC-2ex Heterogeneous Computing Platform,"** ***Workshop on the Intersections of Computer Architecture and Reconfigurable Logic*** **(CARL), December 2013, Davis, CA.**

10. ***Mikhail Kazdagli*****, Ling Huang, Vijay Reddi, Mohit Tiwari, "Morpheus: Benchmarking Computational Diversity in Mobile Malware".** ***Workshop on Hardware and Architectural Support for Security and Privacy*** **(HASP), June 2014, Minneapolis, MN. (held in conjunction with ISCA).**

11. **Akhila Gundu, Gita Sreekumar, Ali Shafiee, Seth Pugsley,** ***Hardik Jain*****, Rajeev Balasubramonian, Mohit Tiwari, "Memory Bandwidth Reservation in the Cloud to Avoid Information Leakage in the Memory Controller".** ***Workshop on Hardware and Architectural Support for Security and Privacy*** **(HASP), June 2014, Minneapolis, MN. (held in conjunction with ISCA).**

ORAL PRESENTATIONS (oral presentations in rank are shown in bold):

1. Mohit Tiwari, "A Small Cache of Large Ranges: Hardware Methods for Efficiently Searching, Storing, and Updating Big Dataflow Tags", MICRO, November 2008, Lake Como, Italy.

2. Mohit Tiwari, "Complete Information Flow Tracking from the Gates Up", ASPLOS, March 2009, Washington D.C., USA.

3. Mohit Tiwari, "Complete Information Flow Tracking from the Gates Up", August 2009, Naval Postgraduate School, Monterey, USA. **(Invited talk)**

4. Mohit Tiwari, "Quantifying the Potential for Program Analysis Peripherals", PACT, September 2009, Raleigh, NC, USA.

5. Mohit Tiwari, "Execution Leases: A Hardware-Supported Mechanism for Enforcing Strong Non-Interference", MICRO, December 2009, New York, USA.

6. Mohit Tiwari, "Crafting a Usable Microkernel, Processor, and I/O System with Strict and Provable Information Flow Security", ISCA, June 2011, San Jose, CA, USA.

7. Mohit Tiwari, "Context-centric Security", HotSec, August 2012. Bellevue, WA, USA.

8. **Mohit Tiwari, "Practical Oblivious Computation in a Secure Processor", UT Austin Computer Science Systems Seminar, September 2013, Austin, TX, USA. (Invited talk)**

9. **Mohit Tiwari, "Practical Oblivious Computation in a Secure Processor", UMD CS Seminar, September 2013, College Park, MD, USA. (Invited talk)**

10. **Mohit Tiwari, "Hardware support for systems security", UT Austin Programming Languages Lunch, April 2014, Austin, TX, USA.**

11. **Mohit Tiwari, "Protecting User Data from Breaches", Seton and Dell Children's Hospital, May 2015, Austin, TX, USA. (invited talk)**

12. **Mohit Tiwari, "Data Security Beyond Encryption and HIPAA Regulations", Exponential Kansas City, September 2015, Kansas City, MO, USA. (invited talk)**

13. **Mohit Tiwari, "Securing Data in Use: Faster Innovation, Better Security", HIMSS Privacy and Security Forum, November 2015, Boston, MA, USA. (invited talk)**

14. **Mohit Tiwari, "Cybersecurity for Embedded Systems", Lockheed Martin Aerospace group, November 2015, Austin, TX, USA.**

15. **Mohit Tiwari, Christine Julien, "Context-centric Security", Laboratory for Telecommunication Sciences, January 2016, College Park, MD, USA. (invited talk)**

16. **Mohit Tiwari, Michael Orshansky, Andreas Gerstlauer, "Cybersecurity for Embedded Systems", UT Austin and Lockheed Martin Aerospace and Missile Systems, April 2016, Austin, TX, USA.**

17. **Mohit Tiwari, "Towards Trustworthy and Robust Behavioral Malware Detectors", Center for Future Architectures e-Workshop, April 2016.**

18. Mohit Tiwari, "Data Security Beyond Encryption and HIPAA Regulations", HIMSS Privacy and Security Forum, May 2016, Los Angeles, CA, USA. (invited talk)

19. Mohit Tiwari, "Future-proofing IoT Security", ACM/IEEE Workshop on Internet of Things at Design Automation Conference (DAC), June 2016, Austin, TX, USA. (invited talk)

20. Mohit Tiwari, "Software-defined Defenses against Hardware Side-channels" in Workshop titled "Who is the major threat to tomorrow's security? You, the hardware designer", June 2016, Austin, TX, USA. (invited talk)

21. Mohit Tiwari, "Future-proofing IoT Security", at ARM Research, July 2016, Austin, TX, USA. (invited talk)

22. Mohit Tiwari, "Software-defined Hardware Security", Keynote at Workshop on Computer-Aided Design and Implementation for Cryptography and Security (CADICS), November 2016, Austin, TX, USA. (invited talk)

22. Mohit Tiwari, "Systems Security Research in the Spark Lab at UT Austin", UT Austin and General Dynamics Meeting, January 2017, Austin, TX, USA.

23. Mohit Tiwari, "Software-defined Security Against Low-level Attacks", National Institute of Standards and Technology (NIST), February 2017, Gaithersburg, MD, USA. (invited talk)

24. Mohit Tiwari, "Software-defined Hardware Security", Texas A&M University ECE Seminar, March 2017, College Station, TX, USA. (invited talk)

25. Mohit Tiwari, "Composable Primitives for Systems Security", Thirteenth International Summer School on Advanced Computer Architecture and Compilation for High-Performance and Embedded Systems (ACACES), 9-15 July 2017, Fiuggi, Italy. (invited instructor)

26. Mohit Tiwari, Michael Orshansky, Andreas Gerstlauer, "Power Modeling for Cybersecurity", UT Austin and Lockheed Martin Annual Review, September 2017, Austin, TX, USA.

27. Mohit Tiwari, "Data-centric Secure Systems", Visa Research, October 2017, Palo Alto, CA, USA. (invited talk)

28. Mohit Tiwari, Michael Orshansky, Andreas Gerstlauer, "Power Modeling for Cybersecurity", Lockheed Martin MFC Office, January 2018, Dallas, TX, USA.

29. Mohit Tiwari, "Software-defined Hardware Security", CS Department and Huawei Systems Lab, UT Austin, March 2018, Austin, TX, USA. (invited talk)

30. Mohit Tiwari, "Mobile Data Containers", UT Austin and General Dynamics Meeting, March 2018, Austin, TX, USA.

31. Mohit Tiwari, "Side- and Covert-Channels: Notes on Research Lifecycle", Plenary Talk at National Science Foundation Workshop on Side- and Covert-Channel Security, March 2018, Washington D.C., USA. (invited talk)

32. Mohit Tiwari, "A Security Plane for Enterprise Systems", UT Austin and General Dynamics meeting, April 2018, Austin, TX, USA.

33. Mohit Tiwari, "A Security Plane for Enterprise Systems", CS Department, Arizona State University, May 2018, Tempe, AZ, USA. (invited talk)

PATENTS:

Issued patents

1. Ryan Kastner, Jason Oberg, Sarah Meiklejohn, Timothy Sherwood, *Mohit Tiwari,* "Method and systems for detecting and isolating hardware timing channels," U.S. patent number US 2014/0259161 A1, issued September 11, 2014. *(licensed).*

   Based on work Mohit Tiwari did as graduate student at UC Santa Barbara. All research Mohit Tiwari conducted at UT Austin is in the public domain.

GRANTS AND CONTRACTS: **Total funding $5,049,282 at UT.**
My share $3,558,282 at UT.

Acronyms in table below (in order of appearance in table):

- **NSF: National Science Foundation**
- **SaTC: Secure and Trustworthy Cyberspace**
- **NSA: National Security Agency**
- **UMD: University of Maryland**
- **CAREER: Faculty Early Career Development Program**
- **C-FAR: Center for Future Architectures Research (https://www.futurearchs.org/)**
- **I-Corps: NSF Innovation Corps**
- **DARPA: Defense Advanced Research Projects Agency**
- **SSITH: System Security Integrated Through Hardware and Firmware**
- **NSF CSR: National Science Foundation Computer Systems Research**

Co-Investigators	Title	Agency	Grant Total	Period
None	"Digital Insertion and Observation Resistant Execution (DIORE)"	NSF SaTC program	$416,000	08/01/13 – 07/31/17
None	"Human Reasoning about Privacy and Security"	NSA Lablet at UMD	$62,726	02/07/14 - 07/31/17
V.J. Reddi	Power Signatures for Mobile Malware Detection	Google Research Award	$50,000 ($25,000 total PI share)	2014
None	"Exo-Core: An Architecture to Detect Malware as Computational Anomalies"	NSF CAREER award	$522,000	03/01/15 - 02/29/20
None	"Architectures to Protect Data in Motion"	C-FAR Center UMichigan	$485,000	05/07/15 – 12/31/17
None	"I-Corps: Trustworthy Cyberspace through Data-security as a Service"	NSF I-Corps	$50,000	09/01/15 - 02/29/16
M. Orshansky, A. Gerstlauer	"Cybersecurity Research on Power Models"	Lockheed Martin	$500,000 ($166,000 total PI share)	10/31/16 - 08/15/18
S. Shakkottai, C. Caramanis	Anomaly Detection for Cloud Radio Access Network (Cloud-RAN)	Huawei	$100,000 ($30,000 total PI share)	2016

None	"Hardware Introspection Mechanisms for Debugging and Security"	Samsung	$100,000	01/31/16 – 06/01/17
S. Shakkottai, C .Caramanis	"SaTC: CORE: Medium: Guarding Noisy Neighborhoods with Weak Detectors"	NSF SaTC	$1,200,000 ($400,000 total PI share)	03/01/17 - 02/29/21
None	Malware Detection	Qualcomm gift, Faculty Award	$125,000	2017
None	Mobile Data Containers	General Dynamics	$166,000	06/30/17 – 08/31/19
None	Ensembles of Moving Target Defenses	DARPA SSITH program	$748,556	10/31/17 - 01/15/21
PI C. Julien	CSR: Medium: Extensible Distributed Systems Solutions for Community Supported Child-Independent Mobility"	NSF CSR #1703497	$400,000 ($200,000 total PI share)	09/01/17 - 08/31/19
Mattan Erez	Fine-grained Contention Detection and Mitigation	Huawei CS Systems Lab	$124,000 ($62,0000 total PI share)	08/01/18 - 07/31/19

PH.D. SUPERVISIONS COMPLETED:

Kazdagli, Mikhail	**June 2018**	**Robust Behavioral Malware Detection**	**Electrical and Computer Engineering**	**The University of Texas at Austin**

M.S. SUPERVISIONS COMPLETED:

Santa Maria, Daniel	June 2017	Identifying post-silicon bugs and their root causes through a hardware introspection engine	Electrical and Computer Engineering	The University of Texas at Austin
Sankaranayanan, Naveena	June 2018	Security evaluation of Linux Containers	Electrical and Computer Engineering	The University of Texas at Austin
Prakash, Rohith	June 2018	Course-based MS. Research: side-channel privacy through input indistinguishability	Electrical and Computer Engineering	The University of Texas at Austin

PH.D. IN PROGRESS:

A. Students admitted to candidacy

Ashay Rane (CS Department, co-advised with Dr. Calvin Lin). *Started PhD in Fall 2012, and working with Dr. Tiwari in Spring 2014.*

B. Post M.S. students preparing to take Ph.D. qualifying exam

Austin Harris. *Started MS/PhD in Fall 2013.*
Sarbartha Banerjee. *Started MS in Fall 2016 at UT ECE, and PhD in Fall 2018 with Dr.Tiwari.*
Willy Ray Vasquez. *Started PhD in Fall 2017.*

C. Ph.D. students preparing to take Ph.D. qualifying exam

Casen Hunger. *Started MS/PhD in Spring 2015.*
Shijia Wei. *Started MS/PhD in Fall 2016.*
Prateek Sahu. *Started MS/PhD in Fall 2017.*

M.S. IN PROGRESS:

Pranav Kumar. *Started MS in Fall 2017*

POSTDOC COMPLETED:

Aydin Aysu (08/22/2016—6/29/2018). **Starting as tenure-track Assistant Professor in ECE Department, North Carolina State University (NCSU) from Fall 2018.**

VITA: Mohit Tiwari received a Bachelor of Technology degree in Computer Science and Engineering from the Indian Institute of Technology, Guwahati in 2005, and the MS and Ph.D. degrees in Computer Science from the University of California at Santa Barbara (UCSB) in 2010 and 2011, respectively. His research at UCSB received the Outstanding Dissertation Award and has subsequently been commercialized by his mentees through an NSF-funded corporation (Tortuga Logic). He then won the NSF Computing Innovation Fellowship (2011 – 2013) to work as a post-doctoral scholar with Prof. Krste Asanovic and Prof. Dawn Song at University of California, Berkeley. Mohit Tiwari joined the faculty of UT Austin ECE in August 2013 as an assistant professor where he currently is a Fellow of the AMD Chair. His research focuses on computer architectures and systems for cybersecurity and privacy. His research awards include the Qualcomm Faculty Award, the National Science Foundation CAREER award, Best Paper Awards at ASPLOS'15, PACT'09, and (runner-up at) HOST'18, IEEE Micro Top Picks of year in computer architecture (2010, 2015 Honorable Mention), and the CSAW top-10 Best Applied-security Paper in Cybersecurity in 2013, while his undergraduate research students have received the Marjorie Morales and NSF/SRC awards for excellence in research.

Candidate's Summary of Activities
Mohit Tiwari
Assistant Professor, ECE Department
UT Austin

Metric	Value
Peer-reviewed journal publications (in rank and total) ***	2+1 / 6+1
Peer-reviewed conference proceedings (in rank and total)	12 / 22
Number of journal papers in rank with supervised student(s) and/or post-docs from UT as co-author(s) ***	***1 + 1***
Number of journal papers in rank with supervised student(s) from UT as co-author ***	1 + 1
Total citations of all publications (career) from ISI Web of Knowledge *****	178
Largest number of citations for a single paper based on work at UT (ISI Web of Knowledge) *****	***29***
h-index (career) from ISI Web of Knowledge *****	7
Total citations of all publications (career) from Google Scholar (as of July 28, 2018)	1150
Largest number of citations for a single paper based on work at UT (Google Scholar)	***145***
h-index (career) from Google Scholar	18
Total external research funding raised in rank	$ 5.05M
Total external research funding raised in rank (candidate's share)	$ 3.56M
Total number of external grants/contracts awarded in rank	15
Number of external grants/contracts awarded in rank as PI	14
PhD students completed (***sole supervisions and co-supervisions)†***	***1 / 0***
MS students completed ***(sole supervisions and co-supervisions)†***	***3 / 0***
PhD students in pipeline ***(sole supervisions and co-supervisions*** as of ***8/31/2018***) †	***6 / 1***
MS students in pipeline ***(sole supervisions and co-supervisions*** as of ***8/31/2018***) †	***1 / 0***
Number of courses taught	8
Total number of students taught in organized courses	291
Average instructor rating for undergraduate courses	4.05
Average instructor rating for graduate courses	4.25
Average course rating for undergraduate courses	3.85
Average course rating for graduate courses	4
Number of teaching awards	0
Student organizations advised	0
Undergraduate researchers supervised *******	13 + 1
Service on journal editorial boards	2
Number of symposia organized	1

NOTES:

*** +1: invited paper to Transactions on Computer Science (TOCS) based on ASPLOS'15 Best Paper Award ("Ghostrider: A hardware-software system for memory trace oblivious computation"). The paper has been invited and pre-accepted but it is in preparation and hence not listed in the CV.

***** ISI Web of Knowledge is missing crucial papers (#2 and #8 from Google Scholar ordered by citation count, and likely others); it has far lower citation counts than Google Scholar for the same papers, and has a different set of papers when ordered by citation count.

******* Undergraduate researchers list comprises of 11 funded summer and school-year positions, 2 unfunded students, and +1 is an undergraduate from Rice University.

Complete reverse chronological list of publications and scholarly/creative works
Mohit Tiwari

Title of Dissertation: Design and Verification of Information Flow Secure Systems
Dissertation Advisor: Dr. Timothy P. Sherwood

Section 1. Works published (or in an equivalent status), in press, accepted, or under contract while in current rank at UT Austin.

Note: my advisees/students are highlighted in italic – please see my CV for a complete list and criteria used to identify my students.

Refereed archival journal publications in rank

1. Pavel Lifshits, Roni Forte , Yedid Hoshen, *Matthew Halpern, Manuel Philipose*, Mohit Tiwari, and Mark Silberstein, "Power to peep-all: Inference Attacks by Malicious Batteries on Mobile Devices", in Proceedings on Privacy Enhancing Technologies (PoPETs), July 2018.
   - Co-authors: Pavel Lifshits (Research Engineer at Technion Israel Institute of Technology), Roni Forte (student, Technion Israel Institute of Technology), Yedid Hoshen (doctoral student, Hebrew University), Matthew Halpern (doctoral student, UT Austin), Manuel Philipose (B.S., UT Austin), Mark Silberstein (faculty peer at Technion Israel Institute of Technology)
   - Qualitative statement of contribution: I started the project on using programmable batteries (more generally, the power draw of a system on chip) to leak sensitive data with Matthew Halpern and Manuel Philipose in UT Austin as graduate course projects in 2013 and 2014 fall. We focused on information leaks through web browsers and leak-prevention using dynamic voltage frequency scaling, while (2015 fall onwards) Technion and Hebrew University colleagues focused on keystroke recognition and camera detection. I co-designed the studies and co-wrote the paper along with last author (Mark Silberstein) while our students carried out the experiments.

2. Wei Hu, Dejun Mu, Jason Oberg, Baolei Mao, Mohit Tiwari, Timothy Sherwood, Ryan Kastner, "Gate Level Information Flow Tracking for Security Lattices," ACM Transactions on Design Automation of Electronic Systems (TODAES), Volume 20, November 2014.
   - Co-authors: Wei Hu (post-doctoral scholar, UC San Diego), Dejun Mu (faculty peer, Northwestern Polytechnical University), Jason Oberg (graduate student, UC San Diego), Baolei Mao (graduate student, Northwestern Polytechnical University), Timothy Sherwood (faculty peer, UC Santa Barbara), Ryan Kastner (faculty peer, UC San Diego)
   - Qualitative statement of contribution: I introduced the precise information flow tracking algorithm for general lattices in my dissertation. My colleagues in San Diego evaluated this algorithm for a range of hardware designs and wrote this journal paper.

Refereed conference proceedings in rank

1. *Aydin Aysu, Youssef Tobah*, Mohit Tiwari, Andreas Gerstlauer, Michael Orshansky, "Horizontal Side-Channel Vulnerabilities of Post-Quantum Key Exchange Protocols," Proceedings of IEEE

International Symposium on Hardware Oriented Security and Trust (HOST), May 2018, Washington DC, USA. **(Best Paper Award, Runner-up).**

- Co-authors: Aydin Aysu (post-doctoral scholar, UT Austin), Youssef Tobah (undergraduate student, UT Austin), Andreas Gerstlauer (faculty peer, UT Austin), Michael Orshansky (faculty peer, UT Austin)
- Qualitative statement of contribution: I co-designed the study of information leaks in quantum computing resistant cryptographic key-exchange algorithms (together with Andreas Gerstlauer and Michael Orshansky). We share with our post-doctoral scholar, Aydin Aysu, the credit for designing experiments, developing countermeasures, and writing the paper. Youssef Tobah and Aydin Aysu implemented the countermeasures in hardware and did all the experiments.

2. *Casen Hunger*, *Lluis Vilanova*, Charalampos Papamanthou, Yoav Etsion, Mohit Tiwari, "DATS: Data Containers for Web Applications," Proceedings of Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2018, Williamsburg, VA. **(Awarded NSF I-Corps award to evaluate commercialization opportunities; piloted by cloud providers)**

- Co-authors: Casen Hunger (graduate student, UT Austin), Lluis Vilanova (post-doctoral scholar, Technion), Charalampos Papamanthou (faculty peer, University of Maryland), Yoav Etsion (faculty peer, Technion).
- Qualitative statement of contribution: I and my student Casen Hunger developed the DATS design pattern for web-applications, designed experiments to test the security, programmability, and performance of DATS, and wrote/revised drafts the paper. Casen is the lead developer of the DATS system. Lluis Vilanova visited my lab in Fall 2014 -- he helped implement the first version during Fall 2014 and (since then) co-wrote drafts of the paper. Drs. Papamanthou and Etsion gave feedback on the design and paper-drafts of the DATS system.

3. Aydin Aysu, Michael Orshansky, Mohit Tiwari, "Binary Ring-LWE Hardware with Power Side-Channel Countermeasures," Proceedings of Design Automation and Test in Europe (DATE), March 2018, Dresden, Germany.

- Co-authors: Aydin Aysu (post-doctoral scholar, UT Austin), Michael Orshansky (faculty peer, UT Austin)
- Qualitative statement of contribution: I co-designed the study of information leaks in quantum computing resistant cryptographic encryption/decryption algorithms, co-designed the algorithms to mitigate these leaks, and co-wrote the paper together with Aydin Aysu and Michael Orshansky. Aydin Aysu implemented the algorithms in hardware.

4. Ali Shafiee, Rajeev Balasubramonian, Mohit Tiwari, Feifei Li, "Secure DIMM: Moving ORAM Primitives Closer to Memory," Proceedings of International Symposium on High Performance Computer Architecture (HPCA), February 2018, Vienna, Austria.

- Co-authors: Ali Shafiee (graduate student, University of Utah), Rajeev Balasubramonian (faculty peer, University of Utah), Feifei Li (faculty peer, University of Utah)
- Qualitative statement of contribution: I helped with the design of Secure DIMM and with writing paper drafts. Ali Shafiee and Rajeev Balasubramonian led the design and implementation of the system.

5. *Mikhail Kazdagli*, Vijay Janapa Reddi, Mohit Tiwari, "Quantifying and Improving the Efficiency of Hardware-based Mobile Malware Detectors," Proceedings of the 49th International Symposium on Microarchitecture (MICRO), October 2016, Taipei, Taiwan. **(Transitioned to Qualcomm Malware Research team, led to Qualcomm Faculty Award 2017.)**

- Co-authors: Mikhail Kazdagli (graduate student, UT Austin), Vijay Janapa Reddi (faculty peer, UT Austin)
- Qualitative statement of contribution: I and my student, Mikhail Kazdagli, designed the Sherlock system introduced in the paper, and co-wrote drafts of the paper. Mikhail built the system. Dr. Reddi is an expert in mobile computing and provided extensive feedback on the system design and paper drafts. Mikhail transitioned ideas from this paper to Qualcomm over an 8-month internship, was awarded a patent with them, and was responsible for my Qualcomm Faculty Award in 2017.

6. *Ashay Rane*, Calvin Lin, Mohit Tiwari, "Secure, Precise, and Fast Floating-Point Operations on x86 Processors," Proceedings of the 25th Usenix Security Symposium, August 2016, Austin, TX.

- Co-authors: Ashay Rane (graduate student, UT Austin), Calvin Lin (faculty peer, UT Austin CS Department)
- Qualitative statement of contribution: I and Dr. Lin co-designed and co-wrote the Escort system described in the paper with Ashay Rane, our co-advised student. Ashay Rane built the compiler transformations and ran the extensive evaluations for this project.

7. *Ashay Rane*, Calvin Lin, Mohit Tiwari, "Raccoon: Closing Digital Side-Channels through Obfuscated Execution," Proceedings of the 24th USENIX Security Symposium, August 2015, Washington, D.C.

- Co-authors: Ashay Rane (graduate student, UT Austin), Calvin Lin (faculty peer, UT Austin CS Department)
- Qualitative statement of contribution: I and Dr. Lin co-designed and co-wrote the Raccoon system described in the paper with Ashay Rane, our co-advised student. Ashay Rane built the compiler transformations and ran the extensive evaluations for this project.

8. *Ali Shafiee*, Akhila Gundu, Manjunath Shevgoor, Rajeev Balasubramonian, Mohit Tiwari, "Avoiding Information Leakage in the Memory Controller with Fixed Service Policies," Proceedings of the 48th International Symposium on Microarchitecture (MICRO), December 2015, Waikiki, HI.

- Co-authors: Ali Shafiee (graduate student, University of Utah), Akhila Gundu (graduate student, University of Utah), Manjunath Shevgoor (graduate student, University of Utah), Rajeev Balasubramonian (faculty peer, University of Utah)
- Qualitative statement of contribution: I co-designed the Fixed Service memory controller described in the paper and co-wrote the paper. Ali Shafiee and his advisor Rajeev Balasubramoniam led the design, implementation, and paper writing, with assistance from Akhila and Manjunath in running the experiments.

9. Chang Liu, *Austin Harris*, Martin Maas, Michael Hicks, Mohit Tiwari, Elaine Shi, "GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation," Proceedings of the 15th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2015, Istanbul, Turkey. **(Best Paper Award.)**

- Co-authors: Chang Liu (graduate student, University of Maryland), Austin Harris (graduate student, UT Austin), Martin Maas (graduate student, UC Berkeley), Michael Hicks (faculty peer, University of Maryland), Elaine Shi (faculty peer, University of Maryland)
- Qualitative statement of contribution: In this paper, I and my student Austin Harris introduced the idea of a processor whose micro-architectural timing, external memory access trace, and cryptographically oblivious memory (ORAM) banks are explicitly controlled by software. Austin Harris built the processor hardware with advice from Martin Maas on integrating

ORAM hardware with the processor. I worked with Dr.Hicks and Dr.Shi ,whose student Chang Liu wrote the software, to expose the processor and memory controller to a compiler. The GhostRider hardware-software paper was **invited as a fast-track publication to the Transactions on Computer Systems journal.**

10. *Casen Hunger, Mikhail Kazdagli*, Ankit Rawat, Alex Dimakis, Sriram Vishwanath, Mohit Tiwari, "Understanding Contention-driven Covert Channels and Using Them for Defense", Proceedings of the International Symposium on High Performance Computer Architecture (HPCA), February 2015, San Francisco, CA.

- Co-authors: Casen Hunger (graduate student, UT Austin), Mikhail Kazdagli (graduate student, UT Austin), Ankit Rawat (graduate student, UT Austin), Alex Dimakis (faculty peer, UT Austin), Sriram Vishwanath (faculty peer, UT Austin).
- Qualitative statement of contribution: I and Casen Hunger generalized a large number of information leaks in shared processors as being *contention-driven channels.* Together with Dr. Vishwanath, we started explicitly evaluating contention channels in processors as communication channels; Dr. Dimakis led the formal modeling of contention channels; Mikhail Kazdagli helped implement these channels on Intel x86 hardware; and Ankit Rawat helped measure channel capacity. I co-designed the experiments and co-wrote the paper with all co-authors, while Casen and Mikhail were responsible for the implementation.

11. Xun Li, Vineeth Kashyap, Jason Oberg, Mohit Tiwari, Vasanth Rajarathinam, Ryan Kastner, Timothy Sherwood, Ben Hardekopf, and Frederic Chong, "Sapper: A Language for Hardware-Level Security Policy Enforcement," Proceedings of the 14th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), March 2014, Salt Lake City, UT. **(IEEE Micro Top Picks of the Year in Architecture, Honorable Mention.)**

- Co-authors: Xun Li (graduate student, UC Santa Barbara), Vineeth Kashyap (graduate student, UC Santa Barbara), Jason Oberg (graduate student, UC San Diego), Vasanth Rajarathinam (graduate student, UC Santa Barbara), Ryan Kastner (faculty peer, UC San Diego), Timothy Sherwood (faculty peer, UC Santa Barbara), Ben Hardekopf (faculty peer, UC Santa Barbara), Frederic Chong (faculty peer, UC Santa Barbara)
- Qualitative statement of contribution: I introduced the Sapper hardware design language for dynamic information flow control as a graduate student in UC Santa Barbara, wrote the paper for its first submission. I worked with Xun Li who led the Sapper compiler implementation and Ben Hardekopf, who led the type system specification. Xun and Ben led the writing for the final submission. Subsequently, Vasanth Rajarathinam incorporated a floating point unit into the processor. Drs. Kastner, Sherwood, and Chong provided close feedback for the design and paper drafts.

12. Martin Maas, Eric Love, Emil Stefanov, Mohit Tiwari, Elaine Shi, Krste Asanović, John Kubiatowicz, Dawn Song, "PHANTOM: Practical Oblivious Computation in a Secure Processor", Proceedings of the ACM Conference on Computer and Communications Security (CCS), November 2013, Berlin, Germany. **(NYU-CSAW Best Applied Security Paper of the Year, top-10.)**

- Co-authors: Martin Maas (graduate student, UC Berkeley), Eric Love (graduate student, UC Berkeley), Emil Stefanov (graduate student, UC Berkeley), Elaine Shi (research scientist, UC Berkeley), Krste Asanović (faculty peer, UC Berkeley), John Kubiatowicz (faculty peer, UC Berkeley), Dawn Song (faculty peer, UC Berkeley)
- Qualitative statement of contribution: I introduced the idea of cryptographic obfuscation of memory traces (previously studied as a theoretical primitive to be used with remote servers

over the internet) to the domain of hardware processors. I led the design of the memory controller, its implementation on the Convey Computer's field-programmable gate array (FPGA) server, and wrote the paper. Martin Maas implemented the memory controller and ported SQLite to RISC-V, Eric Love helped run the performance experiments, Emil Stefanov and Elaine Shi consulted with us on the Path ORAM algorithm that we adapted for hardware implementation, and Drs. Asanovic, Kubiatowicz, and Song all gave feedback on paper drafts.

Section 2. Works published (or in equivalent status) while in current rank at other institutions (if applicable)

Not applicable.

Section 3. Works published (or in equivalent status) while in previous rank(s) at UT Austin (if applicable)

Not applicable.

Section 4. Works published (or in equivalent status) while in previous rank(s) at other institutions (if applicable)

Not applicable.

Table 1. Research Summary

Metric	Value
Peer-reviewed journal publications (in rank and total) ***	2+1 / 6+1
Peer-reviewed *(journal-equivalent)* conference proceedings (in rank and total)	12 / 22
Number of journal papers in rank with supervised student(s) and/or post-docs from UT as co-author(s)* ***	1+1
Number of journal papers in rank with supervised student(s) from UT as co-author* ***	1+1
Number of *journal-equivalent conference* papers in rank with supervised student(s) and/or post-docs from UT as co-author(s)*	8
Number of *journal-equivalent conference* papers in rank with supervised student(s) from UT as co-author*	7
Total citations of all publications (career) from ISI Web of Knowledge*****	178
Largest number of citations for a single paper based on work at UT (ISI Web of Knowledge)*****	29
h-index (career) from ISI Web of Knowledge*****	7
Total citations of all publications (career) from Google Scholar *(as of July 1, 2018)*	1119
Largest number of citations for a single paper based on work at UT (Google Scholar)	143
h-index (career) from Google Scholar	18
Total external research funding raised in rank (personal/total for UT)	$3.56M/$5.05M

NOTES:
*** +1: invited paper to Transactions on Computer Science (TOCS) based on ASPLOS'15 Best Paper Award ("Ghostrider: A hardware-software system for memory trace oblivious computation").

***** ISI Web of Knowledge is missing crucial papers (#2 and #8 from Google Scholar ordered by citation count, and likely others); it has far lower citation counts than Google Scholar for the same papers and has a different set of papers when ordered by citation count.

Table 2. Current External Grants and Contracts

Role of Candidate and Co-Investigators	Title	Agency	Project Total	Candidate's Share	Grant Period
PI: Mohit Tiwari	CAREER: Exo-Core: An Architecture to Detect Malware as Computational Anomalies	NSF CAREER	522,000	522,000	2015—2020
PI: Mohit Tiwari	SaTC: CORE: Medium: Guarding Noisy Neighborhoods with Weak Detectors	NSF	1,200,000	400,000	2017—2021
Co-PIs: Sanjay Shakkottai, Constantine Caramanis					
PI: Christine Julien	CSR: Medium: Extensible Distributed Systems Solutions for Community Supported Child-Independent Mobility	NSF	400,000	200,000	2017—2019
Co-PI: Mohit Tiwari					
PI: Mohit Tiwari	Cyber Security Research on Power Models	Lockheed Martin	500,000	166,000	2016—2018
Co-PIs: Michael Orshansky, Andreas Gerstlauer					
PI: Mohit Tiwari	Mobile Data Container	General Dynamics	166,000	166,000	2017—2019
PI: Mohit Tiwari	Ensembles of Moving Target Defenses for Scalable and Composable Hardware Security	DARPA	748,556	748,556	2018—2021
PI: Mohit Tiwari	Fine-Grained Contention Detection and Mitigation	Huawei-CS Systems Lab	124,000	62,000	2018—2019
Co-PI: Mattan Erez					
PI: Mohit Tiwari	PSigns: Power Channels for Malware Detection	Google award	50,000	25,000	gift
Co-PI: Vijay Reddi					
PI Mohit Tiwari	Hardware-based Malware Detection, Faculty award	Qualcomm award	125,000	125,000	gift
PI: Mohit Tiwari	Anomaly Detection for Cloud Radio Access Network	Huawei-WNCG	100,000	30,000	WNCG gift
Co-PIs: Sanjay Shakkottai, Constantine Caramanis					
Total			**3,935,556**	**2,444,556**	

Table 3. External Grants and Contracts Awarded in Rank and Completed

Role of Candidate and Co-Investigators	Title	Agency	Project Total	Candidate's Share	Grant Period
PI: Mohit Tiwari	TWC: Medium: Collaborative Research: DIORE: Digital Insertion and Observation Resistant Execution	NSF	416,000	416,000	2013—2017
PI: Mohit Tiwari	Establishing a Science of Security Research Lablet at The University of Maryland - Human Reasoning about Privacy and Security	NSA	62,726	62,726	2014—2017
PI: Mohit Tiwari	Hardware Introspection Mechanisms for Debugging and Security	Samsung	100,000	100,000	2016—2017
PI: Mohit Tiwari	I-Corps: Trustworthy Cyberspace through Data-security as a Service	NSF	50,000	50,000	2015—2016
PI: Mohit Tiwari	Architectures to Protect Data in Motion	C-FAR Center at University of Michigan	485,000	485,000	2015—2017
TOTAL			**1,113,726**	**1,113,726**	

Table 4. Pending External Grants and Contracts

Role of Candidate and Co-Investigators	Title	Agency	Project Total	Candidate's Share	Grant Period
PI: Mohit Tiwari (UIUC Co-PI: Chris Fletcher)	Intel ISRA: Oblivious Instruction Set Architectures	Intel	300,000	300,000	2018—2021
PI: Mohit Tiwari (UIUC Co-PI: Chris Fletcher)	SaTC: CORE: Small: Collaborative: Oblivious ISAs for Secure and Efficient Enclave Programming	NSF	500,000	250,000	2018—2021
PI: Mohit Tiwari	Mobile Data Containers Year 2	General Dynamics	217,000	217,000	2018—2019
PI: Mohit Tiwari	Cyber Security Research on Power Models	Lockheed Martin	250,000	83,000	2018—2019
Co-PIs: Michael Orshansky, Andreas Gerstlauer					
TOTAL			**1,267,000**	**850,000**	

Mohit Tiwari

Budget Council Statement on Teaching for Faculty Promotion Candidate Mohit Tiwari

This assessment of Assistant Professor Mohit Tiwari's teaching contributions was prepared by Budget Council Member Professor Jonathan Valvano.

Principal area of teaching.
Dr. Tiwari's principal area of teaching is in computer engineering in general and architecture, security, and embedded systems in specific. As an assistant professor, he has taught three different courses: two lower division required undergraduate classes and one advanced graduate class.

Evaluation process.
I based this statement on review of Dr. Tiwari's teaching statement and portfolio, personal experiences, in-class peer evaluations, student course/instructor evaluations for the last five years, as well as my own first-hand experience working together teaching different sections of the same class and my understanding of curricular matters because of my role on the ECE curriculum committee and as undergraduate advisor. I also personally observed his class on 3/6/2017 and 3/19/2018. I have co-taught EE319K with Professor Tiwari three times, and in so doing I have sat in EE319K planning/TA meetings with him dozens of times.

Teaching Evaluation Procedures and Measures
The department uses course evaluation surveys and peer evaluations. It is normal practice to conduct official course evaluations at the conclusion of every class. In spring semesters, EE319K is a large enrollment class with 5 sections. I was one of the instructors Spring 2015, Spring 2016, and Spring 2018 along with Professor Tiwari. Since we have shared homework, shared labs and shared exams, I can attest that Professor Tiwari's students were well-taught each of these three semesters. I think his teaching evaluations capture an accurate representation of his teaching.

Peer evaluations are conducted nominally once per academic year. Peer evaluations are made by tenured professors after a visit to the classroom. The times and dates of these visits are agreed to beforehand so that there are no surprise visits.

- Professor Valvano observed EE319K, Embedded Systems during Spring 2015
- Professor Akinwande observed EE319K, Embedded Systems during Spring 2016
- Professor Valvano observed EE319K, Embedded Systems during Spring 2017
- Professor Valvano observed EE319K, Embedded Systems during Spring 2018

Summary of Teaching Evaluations
The main indicator on the Course Evaluation Surveys used to evaluate teaching performance is the Overall Instructor Rating. His in-rank instructor ratings are summarized in Table 1. The GPA for EE319K, the undergraduate required class, is purposely adjusted to be about 3.0 for all sections. Also, this GPA is consistent with other classes at this level. Therefore, I believe there is no bias in evaluation scores caused by

perceived grade expectations. The average size of his graduate class is 14 students, slightly less than equal to the department average of 17.6.

His weighted average undergraduate instructor rating is 3.98 out of 5, and his weighted average graduate rating is 4.22 out of 5. His performance is less than the department average for undergraduate courses (Spring 2018 ECE average = 4.22) and slightly below the department average for graduate courses (Spring 2018 ECE average = 4.46). In summary, his undergraduate ratings are acceptable and his graduate instructor ratings are excellent.

Semester	Course	#Answered / #Enrolled	Overall instructor rating	Overall course rating
Spring 2015	EE 319K	26/41	3.8	3.6
Spring 2016	EE 319K	30/39	4.3	4.2
Spring 2017	EE 319K	18/78	3.5	3.3
Spring 2018	EE 319K	42/61	4.6	4.3
Spring 2015	EE309K	15/16	3.6	4.0
Fall 2013	EE 382V	9/9	4.5	4.5
Fall 2014	EE 382V	10/18	4.0	3.9
Fall 2015	EE 382V	13/19	4.2	3.8
Fall 2017	EE 382V	23/26	4.3	3.8

Table 1. CIS results for undergraduate and graduate teaching. EE319K is Introduction to Embedded Systems, EE309K is System Security. and EE382V is Security Hardware-Software Interfaces.

Example negative comments from his CIS (undergrad EE309K)

"Rarely showed up for class" (EE309K was team taught)

EE309K was not a traditional lecture course. EE309K was the number that ECE students used when taking the freshman research initiative stream involving system security. Dr Tiwari was involved in organizing this effort, but was not the lead teacher. The CIS numbers reflect that the students felt positive about the opportunity but may have been confused on how to rate Dr. Tiwari as the instructor. Including just his EE319K courses, his weighted undergraduate instructor CIS average is 4.01.

Typical positive comments from his CIS (undergrad EE319K)

"learned a lot"
"constantly challenged us with class problems"
"awesome"
"lectures were great and well organized"
"super approachable"

"very approachable"
"knowledgeable and excited about course material"
"encouraged to take control of my own learning"
"cares about his students"
"extremely passionate about both the course material and helping students learn"

Typical negative comments from his CIS (undergrad EE319K)
"covering more material from labs would be beneficial"
"not well-structured"
"put more emphasis on lab related course material"
"he has bad handwriting"
"the first lectures were good, the quality continually declined; do not regret skipping"

Typical positive comments from his CIS (grad EE382V)
"Enthusiastic"
"Learned a lot"
"Explains very clearly"
"was very effective"
"enjoyed the discussions"
"one of the best teachers so far"

Example negative comments from his CIS (grad EE382V)
"Much of the material… went over my head"
"This course was incredibly difficult and time consuming"
"Labs were disorganized, but I learned from them"
"could be more structured"
"need to be more organized"

Summarizing quotes from Professor Valvano's Spring 2015 visit (exact date unknown)
"Lectures are extremely engaging. He gives a high-level overview of what they will be learning and how the educational components fit together. During lecture, he can get lost in the calculations and would benefit by working out the details in advance."

Summarizing quotes from Professor Akinwande's in class visit. April 6, 2016
"He spoke in a very casual sense that was very interactive with the students and approachable. The instructor repeated student questions to ensure it was clear to all. The lecture was often very interactive in that many students could respond to or ask questions without the need to raise hands. It was a very engaging lecture on Analog to Digital conversion and Sampling theorem. Examples were solved together in class. There were also in-class practice programming functions. Afterward, the programming concepts and methods were discussed collectively."

Summarizing quotes from Professor Valvano's in class visit. March 6, 2017
"He used a mixture of PowerPoint slides and blackboard. The students were very engaged with the game example and later, they were engaged with the prospect of creating sound. Students felt safe to ask and answer questions." *Negatives*:

> "Write things on the board you want them to copy into their notes. Your message on the blackboard can be scattered."

Summarizing quotes from Professor Valvano's in class visit. March 19, 2018

> "He was very positive responding to students ("great, great, great", "that is wonderful", smiling, "great, that is a very good question"). His delivery was articulate. He used PowerPoint slides for structure, but wrote a lot on the white board. He paused frequently and asked for questions. He did an in-class short quiz to see if students understood the key concepts (just 5 minutes). The professor and TAs walked around answering questions." *Negatives*: "White board management and size of writing. From the weekly meetings, I see he teaches more basic fundamentals rather than delve into the details of how to execute lab assignments. Consequently, his students may learn more, but require more effort to figure out stuff on their own (and may have contributed to the lower scores)."

Response to Student and Peer Evaluation Leads to Continuous Improvement

There are not a lot of negative comments about Professor Tiwari's teaching, but one theme that exists is his lecture organization. Both peer review and student evaluations suggest he work on organizing his lectures. When he made adjustments to his lecture, the response was positive.

One of the difficult concepts in EE319K is teaching C programming to students with no prior programming experience other than EE306/BME303. Basically, the problem is there are some students with extensive programming experience and others who just have this one prerequisite class (EE306/BME303) on assembly programming and computer architecture. Professor Tiwari approaches teaching software design first by example and then by having students work exercises in class. His students appreciated his desire to make them think beyond the details of the course.

Teaching Portfolio

There are three aspects of Professor Mohit Tiwari's teaching portfolio that demonstrate he is an effective and passionate educator. First, it is clear he cares about his students individually. He demonstrates a sincere desire that they learn, and rejoices when they do. Second, he is willing to experiment with his teaching style. He not only tries new approaches but also evaluates the outcomes of the effort to know what works and what doesn't work. Third, he has a fundamental grasp of both the level of our student population and what our students need to be successful in their careers. He uses these incites to design an effective approach when teaching his courses.

Comparison to Other Assistant Professors in the Department:

The CIS scores for Dr. Tiwari are slightly lower than the other assistant professors. However, his teaching service (new course on security, and the freshman research initiative stream) place him on or above efforts from other assistant professors in the department.

Describe participation on graduate committees

Professor Mohit Tiwari has one PhD student who passed the defense. He has one PhD student in candidacy. He has eight PhD-bound students in the pipeline. He supervised three MS thesis students in rank that have graduated.

Conclusions

There are many dimensions to the teaching contributions of a professor, some measurable quantitatively, some measurable qualitatively. On every dimension, Professor Tiwari's contributions put him well above the bar: his approach to teaching not only what but why, his passion for getting students to learn, his mentoring of individual students, his desire to improve his classroom teaching skills, and his constant desire to innovate his teaching. Professor Tiwari demonstrates the excellence that clearly supports this promotion.

Summary prepared by Budget Council Member Professor Jonathan Valvano.

Jonathan W. Valvano

Jonathan Valvano

Mohit Tiwari **Teaching Statement** June 2018

I have been immensely inspired by great teachers. I know first-hand that a great teacher can bring a subject alive, and at the same time, impart values to do research and live by. As a professor at UT Austin, I have the privilege to grow as a teacher and a mentor both by working with students and by team-teaching a course with some of the best teachers in our department. In this statement, I will discuss the key principles and results from my teaching experience, and close with the plan for a four-semester cyber-security course sequence that I am helping to establish at UT Austin.

1 Undergraduate teaching: Embedded Systems

Course Description. I teach the undergraduate freshman course EE 319K, 'Introduction to Embedded Systems'. This course is taken by students in their second semester and it ties computer organization, imperative programming, and signal processing together into an extremely fast-paced lab-based course. The students end with a competition where they design a game from scratch—including the graphics, sounds, user-inputs, game-logic, and UART networking for multi-board games—and evaluate their peers' games to decide the best games. The top two teams in each section (40–80 students) compete with the top teams from the overall class (of about 350 students). This class is unique—instead of boards like Raspberry Pi that hide the hardware through libraries and emphasize either programming or sensor-interfacing, EE 319K keeps both of these in scope and adds human users (who play the games and award points for games being "fun to play") into consideration. EE 319K thus gives students their first end-to-end system-building experience.

Teaching goals. The primary theme I emphasize is that computer engineering is undergoing a radical transformation and EE 319K concepts are at the heart of it. CMOS technology scaling is slacking off, new computational media mesh storage and computation in fundamental ways, and computers are being used in national elections and self-driving cars—clearly, engineers who can change everything from human abstractions and algorithms to compilers and hardware will fuel our society's future. Hence, I emphasize that simply learning EE 319K material to solve exam problems will only get them a good grade—if they want to have impact, and have my entire research lab help them with internships or undergraduate research, they have to use fundamental concepts creatively. For example, they can structure their game engine as a principled state machine (instead of spaghetti logic); make interesting computation vs. memory trade-offs; use professional software development processes; put motion-sensors to creative uses for their game; or iterate their game's design and implementation enough times that the game is "fun" to play. I bring in students from previous years to give tips on how to design and engineer games, institute awards for technical achievement and code-quality (in addition to the best overall game), and run several additional working sessions with TAs and myself outside of lecture hours.

Furthermore, I specifically aim to train students who are new to programming reach the productivity levels of students who have programmed in high school. The key idea is to get students comfortable with abstractions (network layers are a great case-study), to emphasize the importance of principled control flow (state machines in 319K) and data structures to structure programs (vs. thinking in loops and conditionals as imperative languages encourage), and to explicitly write correctness invariants for functions and loops (as opposed to writing quick and dirty code that is intended to be cleaned up using debuggers). To really learn fundamental concepts, I use several small in-class problems that access prior concepts in new situations. I am encouraged to see that every year, one of the top two teams from my section that goes to inter-section "super-finals" has students who had no serious programming experience beyond the Introduction to Computing (EE 306) course.

Outcomes. The outcome of these teaching techniques is that several undergraduates want to sign up for research—I advise 3–5 extremely motivated students on undergraduate research every summer based on their performance in EE 319K. I give strong written/verbal references for several students who intern at top companies (Google, ARM, Qualcomm, etc) and national labs. Over time, as I have become better at communicating that lectures and labs are merely starting points, my student-feedback scores have risen from 3.8 in my first stint to 4.6 in my fourth and most recent stint (the average/median/90th percentile ratings for EE 319K are 3.9/4.1/4.3). In two out of four years, student projects from my section have been rated the best game across all five sections.

Students' comments and their impact on teaching. I periodically survey students to adapt my teaching. Following my first midterm in Spring'15 (the first time I taught the course), students suggested that using old exams and lecture notes is insufficient to prepare well for exams. Each instructor-mix in 319K produces exams that cover the same fundamentals but in ways that sometimes differ wildly from preceding years. Hence, I started testing students with (sometimes, timed) problems during my lectures. In the next midterm, over 50% of my students scored a 100 on the exam and credited the in-class problems for their improvement. For the following year (Spring'16), I noted from CIS comments that the difficulty of the in-class problems could be tuned better and have refined the problems every year – I do not get this feedback now. Instead, my current focus is on making sure my board work is clearer and helps those who take detailed notes based on what is written on the board.

In Spring'17, my section went from 40 to over 70 and walking around in the class peering into students' computers did not scale well. I heard from students that sometimes those who are further along must wait longer while students who were learning programming for the first time might be missed by my scans. (Note that this feedback is not in the CIS scores from Spring'17 – these were e-filed out of class and hence do not contain feedback from the entire class). To address this limitation, my graduate students and I built software that creates workspaces that instructors have access and each student can program. This will allow me to track everyone's progress, conduct surveys, or watch and debug any student's work collaboratively in real time during lectures. We are piloting this with my graduate class this semester and will use it for 319K next semester.

More conceptually, given the extremely limited time to cover 319K topics, there is a tension between focusing on fundamentals and teaching how to solve lab assignments. I strongly believe that, given the step-by-step lab instructions and the large number of TAs that support EE 319K, students should learn to solve the labs primarily on their own initiative. Instead, I try to use lectures to dive deeper into concepts through problems, and discuss connections with other subjects they will learn in ECE. I make it clear that their primary responsibility is to acquire skills in the lab that will enable them to make a great final project (the game). While this leads to some complaints in CIS comments, I have had several students thank me for this 'project-mode' training once they have done some internships.

Capstone design project. Every year, I advise a team of seniors in their year-long capstone design project. My first 319K students are now seniors and have begun signing up for capstone projects with me. After two years of ambitious projects on building vehicle-to-vehicle networking testbeds, we focused on a simpler project (a home-surveillance system with several different sensors) that we could polish—this project won the best Capstone project award in Spring'18. I am also extremely satisfied that the team that won the best project in the Honors/Entrepreneur category also had 4 (of 5) students from my first 40-person 319K class; and that every one of the six award-winning teams had students that I wrote letters for (or recommended) based on their 319K performance.

Undergraduate Research. I have advised 14 undergraduate students over the last 5 years (primarily as funded summer research interns). The students have been co-authors in top-tier papers (HPCA'15, PETS'18, and HOST'18 Best Paper runner-up), they have won SRC (Semiconductor Research Corporation) fellowship and the UT College of Natural Sciences Marjorie Morales Award for undergraduate research, and four of the ten graduated students have gone on to graduate school.

2 Graduate Teaching: Secure Architectures

Course description. My graduate computer security course (EE 382V) introduces students to how sytems can be attacked and how to architect secure systems. The key theme is to specifically tease out security concepts and demonstrate how they come up in hardware, software, and distributed systems. The course is taught through research papers where we discuss (a) *examples* of complex but critical systems being "hacked," e.g., cars, medical devices, voting machines, mobile phones, and the cloud/data-centers, analyzing the systems' vulnerabilities across computer engineering, socio-economic, and human factors; (b) *formal models* for security including access control models, information flow policies, anonymity through quasi-identifier based policies or differential privacy, and examples of applying these policies to different scenarios; (c) *mechanisms* from VLSI design, computer architecture, operating systems, and compilers to generate randomness and identities, and to ensure isolation and enforce authorization rules, and finally (d) back to examples to see how to compose the mechanisms.

Teaching goals and methods. The coursework currently includes 8 weeks of assignments on basics such as applied cryptography, metadata-based information leaks and fixes, exploiting errors in applications and operating systems, and constructing defenses using operating system (OS) techniques. Two of the five assignments involve student competitions—specifically, to extract secret keys from power traces drawn from FPGAs, and to construct covert channel attacks across virtual machines. Students found these open-ended assignments significantly more exciting than standard ones. The course then launches into a 7 week project where students build a new artifact and write a report (at the level of a workshop paper). Prior projects have used new architectures (like Intel SGX) to improve OS-defenses, new VLSI design tools to protect secret keys (e.g., from power channels), and distributed blockchain-based "smart"-contracts. More generally, the students' goal is to extend a top-tier systems security paper to write a new one. The students write formal reviews for one research paper per class and discuss others' reviews online before the corresponding lecture. The class also includes remote attendees from companies, who we invite to virtual lab-sessions and office-hours, and precocious undergraduates who have done extremely well in other computer systems courses.

Outcomes. Top students from this course have subequently published top-tier papers in security and architecture conferences based on their course projects—beyond the students I recruited into my research group. MS students have used their course projects to get full-time and internship positions on related topics. The course gets an average student-rating of 4.25 in a typical class-size of 20-25 students.

3 Freshman Research Initiative Stream

I introduced a Freshman Research Initiative (FRI) "stream"—i.e., a 3-semester course-sequence—from January 2015 through December 2016. Our systems security stream trained freshmen in research skills—reading papers, writing critiques, conducting experiments, using systems tools, and presenting their work—during Spring semester and had the students work on live research projects with graduate students during Summer and Fall semesters. Thus, FRI truly accomplishes both teaching and research objectives in a uniquely integrated way. FRI has been in existence for almost a decade, and longitudinal tracking data indicate that FRI has multiple important effects. 35% more FRI students graduate than a matched sample of their peers, and 32% of FRI students go on to graduate or professional schools (vs. 9% of non-FRI students).

Teaching methods and goals. The primary objective of FRI is to involve undergraduates in conducting science research from the outset of their college careers. This course was a simplified version of our graduate security course but with my graduate student as the FRI stream's "research educator" (i.e., lead instructor)—together, we set up concepts before reading a top-tier research paper and discussed them as in the graduate EE 382V course[1], worked on almost the same assignments but with a whole semester devoted to them (instead of 8 weeks for graduate students). Some of the students stayed over the summer to do research, while all returned in fall to work with graduate students on a variety of research projects in security. While the 2015 stream had only 2 women in a class of 15, 5 of 16 students in 2016 were women.

Outcomes. Several of the 2015 students did their undergraduate honors thesis on systems security—having finished the stream in their second year of undergraduate studies, they came back to do research in the 2017-18 academic year. (We are conducting a survey to see how the stream affected their studies and final choice of jobs after college). Of the 25 total streams in the College of Natural Sciences, our stream was chosen as one of the 6 spotlight streams in a 10-year anniversary event. The research educator (RE) role in an FRI stream is a unique opportunity for a senior graduate student (or post-doctoral scholar) to learn how to teach—Ashay Rane, our RE, did a fantastic job and will apply for academic positions in Fall'18. Our undergraduate TA, Manuel Philipose, continued to work with us on research and won the Marjorie Morales award for undergraduate research at UT Austin.

4 Computer Security Courses and Operations Lab

Beyond my graduate course, I am working to set up a 4-course sequence in computer security culminating in a capstone course where students learn by securing UT Austin's network of 150,000 machines.

The first course is a meaty introduction targeted at senior undergraduates and first-year graduate students. The goal of this course is to ensure that students understand the basics of cryptography and system security well enough to write and operate web-applications securely. The next two courses are intended for serious security researchers—one course will dive into security topics in programming languages, operating systems, and architecture in a systems-focused course, with the second course focusing on topics in distributed systems such as cryptographic protocols, anonymity, and privacy. Clearly, concepts cross over between the two courses, but this split reflects the difference in tools employed by security work in the PLDI, SOSP, and ISCA communities vs. those used by CRYPTO and PETS communities, even if both communities overlap substantially with the core S&P, CCS, and Usenix security community.

The fourth capstone course will be co-taught with the Chief Information Security Officer (CISO) of UT Austin. Students will put all concepts—including data-science techniques learnt from complementary

[1] Reading list: https://www.cs.utexas.edu/users/fri-security/old/spring-15/papers/

courses in ECE—to defend the 150,000 node UT Austin network. This network generates 4TB of network-traffic logs per day, allows students to bring in arbitrary machines (vs. the locked-down devices that are used in commercial enterprises like Google), and have to run several UT-wide web-services ranging from employee records to laboratory web-sites. This course will provide students with a live test-bed, instead of a passive data-set, to apply theoretical concepts learnt in the previous security courses. In addition, this *Cybersecurity Operations Lab* will serve as an evaluation platform for several research and commercial tools that all claim incredible results on closed data-sets.

This course sequence is part of a broader initiative in UT Austin to build well-rounded security professionals. For example, students can take Robert Chesney's Law and Policy courses that specifically target cyber-security issues. Overall, my goal is to help set up the Cybersecurity Operations Lab and these courses as the backbone of a vigorous cybersecurity program at UT Austin.

Table 1. Summary of Course-Instructor Ratings

Metric	Value
Total number of students taught in organized courses	291
Average instructor rating for undergraduate courses	4.05
Average instructor rating for graduate courses	4.25
Average course rating for undergraduate courses	3.85
Average course rating for graduate courses	4

Table 2. Course Schedule by Semester

Course	F 13	S 14	F 14	S 15	F 15	S 16	F 16	S 17	F 17	S 18
EE 319K		Teaching relief		41		39		78		61
EE 382V	9		18		19		Parental leave		26	

Table 3. Summary of Graduate Students Currently Supervised at UT Austin

Student Name	Co-Supervisor	Degree	Start Date	Date Reached Candidacy	Date Expected to Reach Candidacy	Expected Graduation Date
Austin Harris		MS, PhD	08/2013		Fall 2018	Spring 2019
Ashay Rane	Calvin Lin, CS	PhD	08/2012**	04/2017		Spring 2019
Casen Hunger		PhD	01/2015		Spring 2019	Spring 2020
Shijia Wei		PhD	08/2016		Spring 2019	Spring 2021
Sarbartha Banerjee		MS, PhD	08/2016		Spring 2020	Spring 2022
Willy Vasquez		PhD	08/2017		Spring 2020	Spring 2022
Prateek Sahu		MS, PhD	08/2017		Spring 2020	Spring 2022
Pranav Kumar		MS	08/2017		Spring 2020	Spring 2022

**** Ashay Rane and I started working together in Spring 2014.**

Graduated PhD: Mikhail Kazdagli, Spring 2018.
Graduated MS (research assistants): Daniel Santa Maria, Spring 2017. Naveena Sankaranarayan, Spring 2018. Rohith Prakash, Spring 2018.

Mohit Tiwari
Department of Electrical and Computer Engineering
Course Rating Averages

Mohit Tiwari (mt28295). Assistant Professor. ECE Department.
What source was used to complete this chart? My CIS

EE319K: Introduction to Embedded Systems

Semester	Class Size	Number of Responses	Instructor Rating	Course Rating
Spring 2015	41	26	3.8	3.6
Spring 2016	39	30	4.3	4.2
Spring 2017	78	18*	3.5	3.3
Spring 2018	61	42	4.6	4.3
Mean	**55**	**33**	**4.05**	**3.85**

* CIS forms completed electronically outside of class. Hence the low turnout compared to other years.

EE 382V: Security at the Hardware-Software Interface

Semester	Class Size	Number of Responses	Instructor Rating	Course Rating
Fall 2013	9	9	4.5	4.5
Fall 2014	18	10	4.0	3.9
Fall 2015	19	13	4.2	3.8
Fall 2017	26	23	4.3	3.8
Mean	**18**	**14**	**4.25**	**4.00**

EE309K, CS 378: Systems Security Freshman Research Initiative (FRI) Stream

Semester	Class Size	Number of Responses	Instructor Rating	Course Rating
Spring 2015	16	15	3.6	4.0
Fall 2015	15	3	3.0	3.3
Fall 2016	10	2	5.0	4.5
Mean	**14**	**7**	**3.87**	**3.93**

Note: FRI courses are taught by Research Educator (RE) with me as a mentor. My CIS scores here are thus not representative of my undergraduate teaching.

Course Instructor Survey Results

Name/EID: TIWARI, MOHIT (mt28295)
Department: Elec & Computer Engr
Report Date: 07-10-2018

				Instruction	Enroll-	# of Surveys	Avg. Overall	Avg. Overall
Semester	Unique #	Course #	Course Title	Type	ment	Returned	Instructor Rating	Course Rating
Fall 2013	17315	E E 382V	SECURITY HRDWRE-SFTWRE INTERF	Organized	9	9	4.5	4.5
Fall 2014	17445	E E 382V	SECURITY HRDWRE-SFTWRE INTERF	Organized	18	10	4	3.9
Spring 2015	15763	E E 309K	SYSTEM SECURITY	Organized	16	15	3.6	4
Spring 2015	15980	E E 319K	INTRO TO EMBEDDED SYSTEMS	Organized	41	26	3.8	3.6
Fall 2015	16905	E E 382V	SECURITY HRDWRE-SFTWRE INTERF	Organized	19	13	4.2	3.8
Fall 2015	50920	C S 378	SYSTEM SECURITY-FRI	Organized	15	3	3	3.3
Spring 2016	16145	E E 319K	INTRO TO EMBEDDED SYSTEMS	Organized	39	30	4.3	4.2
Fall 2016	51675	C S 378	SYSTEM SECURITY II-FRI	Organized	10	2	5	4.5
Spring 2017	16195	E E 319K	INTRO TO EMBEDDED SYSTEMS	Organized	78	18	3.5	3.3
Fall 2017	16890	E E 382V	SECURITY HRDWRE-SFTWRE INTERF	Organized	26	23	4.3	3.8
Spring 2018	15415	E E 319K	INTRO TO EMBEDDED SYSTEMS	Organized	61	42	4.6	4.3

Teaching Evaluation of Mohit Tiwari, Spring 2015, EE319K

This evaluation is performed by Jonathan Valvano and is based on EE319K team meetings, individual conversations and interviews with TAs and students.

EE319K, 44 students, Lecture RLM 6.104, MW 300 to 430p

Positives: Lectures are extremely engaging. Student attendance is very high, about 80%. He gives a high level overview of what they will be learning and how the educational components fit together. Furthermore, he gives low level details so students learn not only why but how to develop embedded systems. He has a clear interest and respect for his students and his students have a respect of him.

Negatives: During lecture he can get lost in the calculations and would benefit by working out the details in advance. When I say he sometimes goes off on a tangent, it could also be a positive. However, it is always good to make the connection between the major themes of the lecture to the tangents. From a practical aspect he should work to return graded exams back to his class faster because students are anxious and will learn more from their mistakes when exams are returned promptly. Also when teaching a lab class like EE319K, students benefit from in class demonstration of the tools and the hardware. So I suggest he try more class demos.

Discussion: I met with Professor Tiwari multiple times to discuss teaching in general and EE319K in specific. The dates and times of these meetings were April 13, April 20, and April 27, all at 9am.

Summary: Professor Tiwari is just starting out teaching undergraduates, and has the skills and desire to become a great educator. I was happy to team teach with him and look forward to teaching with him next spring.

Peer Evaluation for Professor Mohit Tiwari

1. Instructor's name: **Mohit Tiwari**

2. Evaluator's name: **Deji Akinwande**

3. Date that the evaluator visits the class: **April 6 2016**

4. Course number and title: **EE319k**

5. Evaluator's signature: Akinwande

6. Date that the evaluator discusses the findings with the instructor: **April 6 2016**

Peer-Observation:

EE319k, or 'Introduction to Embedded Systems' is a 4-credit hours lecture plus lab course taken mostly by freshmen (2nd semester is most common), and is a core course required for all ECE undergraduates. The goal is to provide a hands-on (introductory) experience with both CE and EE parts of the curriculum -- e.g., building digital/analog converter blocks and writing software to interface with such devices and LCD screens directly.

This year, there are 5 concurrent sections. Besides Dr. Tiwari, the other sections are taught by Dr. Valvano, Dr. Yerraballi, and Dr. Reddi. All the sections share homework sets, exams, one official set of lecture slides, and labs (everything excluding lectures themselves). There are 10 labs, one homework per week, 2 mid-terms, and a final.

In the course lecture of the peer-review, the instructor focused on recapping important concepts from previous lectures surrounding analog to digital conversion, Nyquist sampling theorem, etc. There were about 55 students of which around 15-20 were students from other sections interested in attending Prof. Tiwari's section. Most of the students arrived on time.

The instructor started the lecture by opening the floor for questions and reviewing highlights from the last lecture. He spoke in a very casual sense that was very interactive with the students and approachable. Many students conversed in discussing the highlights from previous lecture and recent in-class problem sets. The instructor repeated student questions to ensure it was clear to all. The recap of previous lectures and problem sets lasted about 18min followed by a more detailed review and lecture. The lecture was often very interactive that many students could respond to or ask questions without the need to raise hands. It was a very engaging lecture on Analog to Digital conversion and Sampling theorem. Examples were solved together in class.

In terms of teaching technique, the instructor combined powerpoint presentations with blackboard analysis to enhance the learning experience of the students. Since the class involves quite a bit of programming in understanding embedded systems, many students had their laptops open so they could examine their codes as the programming issues and details were under discussion. Some of the students appeared to be adjusting their code as class lecture progressed. There were also in-class practice programming functions. Afterwards, the programming concepts and methods were discussed collectively.

Instructor's name: Mohit Tiwari

Evaluator's name: Jonathan Valvano

Date that the evaluator visits the class: March 6, 2017

Course number and title: EE319K Introduction to Embedded Systems

Review:
1. **Describe the course (e.g. required course, lower or upper division)** EE319K is a required freshman-level lab class.

2. **Describe the topics of the particular lecture:** Today, Professor Tiwari taught how to solve finite state machines in C, using struct, strings, and arrays. He used the example of building a game to make the topic more interesting. Next, he introduced interrupts (I like when he snapped his fingers to get their attention). At the end, he introduced the creation of sound. He did a great job explaining creating sound (output) and sensing (input).

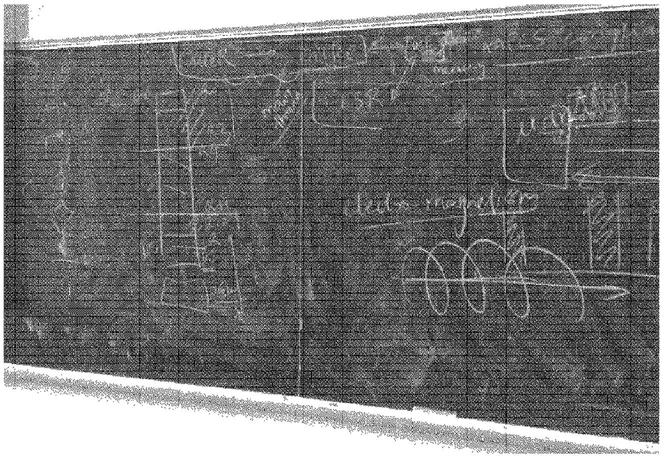
3. **Discuss class attendance (e.g. number of students and whether the students arrive on time):** Attendance was 64 students out of 79 registered, and they arrived on time, ready to learn.

4. **Discuss the instructor's presentation skills (e.g. speaking clearly, the pace of lecture):** Professor Tiwari began with a review of the last class and an overview of the current lecture. He used a mixture of PowerPoint slides and blackboard. The students were very engaged with the game example and later, they were engaged with the prospect of creating sound. He wrote a lot of C code on the board talking about what he was thinking about while he was coding. He gave them a program he wanted them to write and gave them time to work on it. Then, he solved the program on the board. Students felt safe to ask and answer questions.

5. **Discuss the instructor's interaction with the students (e.g. encouraging questions):** He stopped five times during the 75-minute lecture and asked for questions. He had nice pauses after asking a question, giving students time to think. "Does that make sense?" He was very positive when answering questions

6. **Describe students' reactions to the lecture (e.g. engaging):** Students paid attention. Even the students in the back row were taking notes. I interviewed four students after class. All four were very positive, referring to how engaging his lectures are, how respectful he is to students (e.g., when getting their focus back onto lecture), and how well he explains.

Suggestions for improvement: Look at board from back row, maybe adjust the blinds to make it darker. Write things on the board you want them to copy into their notes. One trick other professors use is to write out notes on paper, organize the papers, and then transcribe the paper notes onto the board. This way when you write on the board, what you write on the board will be more organized. Think of students two ways: they are blind and can only hear you (you are good at explaining with your voice); 2) they are deaf and can only see what you write (your message on the blackboard can be scattered). Think of ways to make your boarding writing more organized.



Remember to repeat the question, so other students will better understand your answer. There were two slides that hard to read. I suggest we zoom in the slides that are hard to read. Draw the stack before and after interrupt. Consider printing the "question" you plan to ask in class, and then pass it out. This way everyone knows exactly what you want them to it. Some of the students in the back did not fully understand what being asked.

Date that the evaluator discusses the findings with the instructor (It could be the same day as the visit): We met after class on March 6 4:30pm to discuss the review.

Jonathan W. Valvano
Engineering Foundation Centennial Teaching Fellowship in Electrical Eng (No. 1)
Professor, Undergraduate Advisor
Department of Electrical and Computer Engineering, C0803
University of Texas at Austin,
Austin, TX 78712
voice: 512-471-5141
email: valvano@mail.utexas.edu

Peer Evaluation of Prof. Mohit Tiwari by Prof. Jonathan Valvano

Course Number and Title: ___EE319K Introduction to Embedded Systems_____
Semester: ___Spring 2018____ Type of Course: __ Required Freshman-level _
Enrollment: _50__ Lecture hours/week: __3__ Lab/Recitation hours/week: __1__

1. Pre-Observation Meeting

What is the course content? A class that bridges software design and hardware design involving microcontrollers. On the software side, students program in assembly and C. On the hardware side, students design circuits to interface I/O components like LEDs, switches, sensors, displays, and networks. The analog to digital converter and the digital to analog converter provide the bridge between the hardware and software worlds.

Where does the course fit in the program of study? EE319K is freshman level lab required for all ECE students and some BME students.

Date of Meeting: The pre-observation occurred Monday March 5.

Observations: His biggest concern was organization of lecture. In other words, he wants to improve the structure of each class.

2. Classroom Teaching Observation

Enrollment: **_50_** Attendance: **_42_** Classroom: **_EER1.518_** Start Time: **__1:30p__**

Date of Observation: Monday 19, 2018, 1:30-2:45.

Places of excellence:

Class started on time. He introduced class with informal discussion about class concerning past and future labs. Next, he reviewed fundamental concepts from last time. He exposed both theory and practice. "What is the key insight?" He showed slides and also wrote on the white board. He was **very positive** responding to students ("great, great, great", "that is wonderful", smiling, "great, that is a very good question").

His delivery was articulate. He used PowerPoint slides for structure, but wrote a lot on the white board. He paused frequently and asked for questions. He used a number of techniques to capture attention: changing voice intonation, "this will be 20 points on the next exam", walking back and forth, waving his arms, polling the audience. He makes frequent and appropriate eye contact with students. He was confident and enthusiastic.

He used the PowerPoint slide to transition topics. The slides had a mixture of figures, text and software. The slides were informative, organized, and instructive for the purpose of the lecture.

He did an in-class short quiz to see if students understood the key concepts (just 5 minutes). The professor and TAs walked around answering questions.

He ended class with an extra problem students should work on for next time.

Places for improvement:

The size of his writing on the whiteboard could be larger so it would be easier to read. He should try black or blue markers. The contrast of red is hard to read. When he writes on the board, he should have gone from left to right, when he gets to the end of the board, he should have gone back all the way left and erase.

3. Post-Observation Meeting with Peer Evaluator and Instructor

Date of Post-Observation Meeting: Monday 19, 2018, 3pm. However, because we were team teaching EE319K spring 2018, we met most Mondays at 11am to discuss teaching.

I told him how to get the darker “glass” markers. We discussed organizing his writing on the board. I suggested he look at students notes after class to see what they think they learned from his board writing.

Instructor Strengths

- Enthusiasm
- Communication skills
- Willing to be innovative in teaching
- Interactive
- Respectful

Suggestions for Improvements

- White board management and size of writing
- Color and contrast of markers

4. Interpretation of trends in course instructor survey scores for the instructor

Tiwari, Mohit	2015 Spring	**3.8**
Tiwari, Mohit	2016 Spring	**4.3**
Tiwari, Mohit	2017 Spring	**3.5**

His CIS scores are below average of EE319K instructors (4.2). However, his enthusiasm and willingness to put the effort into teaching is good. He desires to teach this course on a regular basis and desires to improve. From the weekly meetings, I see he tries new approaches to teaching, evaluates the student response. From the weekly meetings, I see he teaches more basic fundamentals rather than delve into the details of how to execute lab assignments. Consequently, his students may learn more, but require more effort to figure out stuff on their own (and may have contributed to the lower scores).

Peer Evaluator ____________________ Date __5/_31_/__2018__

09/06/18
PROGRAM AFPDFGC2

THE UNIVERSITY OF TEXAS AT AUSTIN
OFFICE OF THE PROVOST
COMMITTEE REPORT, MASTERS AND DOCTORAL
FOR TIWARI, MOHIT

PAGE: 1

		LAST		MAST						
		CCYYS	COMM	OR	1ST			2ND		
STUDENT NAME	EID	ENRL	POSITION	DOCT	DEGREE	FIELD	CCYYS	DEGREE	FIELD	CCYYS
ANGEPAT, HARI DAAS	hda73	20189	MEMBER	D						
BANERJEE, SARBARTHA	sb52324	20189	MEMBER	M	M.S.E.	ELECTRICAL AND COM	20182			
CHEN, JIA	jc64546	20189	MEMBER	D						
CHO, SAMUEL SUNGMIN	sc45274	20169	MEMBER	D	PH.D.	ELECTRICAL AND COM	20169			
CHOUKSE, ESHA	ec27876	20189	MEMBER	D						
GUVENILIR, FARUK ALFREDO	fag245	20189	MEMBER	D						
HALPERN, MATTHEW FRANKLIN	mh33338	20172	MEMBER	M	M.S.E.	ELECTRICAL AND COM	20162			
KALBARCZYK, TOMASZ S.	tk7679	20189	MEMBER	D						
KAZDAGLI, MIKHAIL	mk32582	20182	CHAIR	D	PH.D.	ELECTRICAL AND COM	20182			
KHASAWNEH, SHADI TURKI	stk265	20189	MEMBER	D						
LEBEANE, MICHAEL WAYNE	mw1558	20186	MEMBER	D	PH.D.	ELECTRICAL AND COM	20186			
LI, MENG	ml38246	20186	MEMBER	D	PH.D.	ELECTRICAL AND COM	20186			
LIU, CHENGUANG	cl37533	20189	MEMBER	D						
MAXFIELD, COLIN GREGORY	cgm2263	20182	MEMBER	M	M.S.E.	ELECTRICAL AND COM	20182			
NIU, YICHUAN	yn958	20159	MEMBER	D	PH.D.	ELECTRICAL AND COM	20159			
RANE, ASHAY	asr596	20189	CO-CHAIR	D						
SAMYNATHAN, BALAVINAYAGAM	bs33373	20189	CO-CHAIR	D						
SANKARANARAYANAN, NAVEENA	ns28754	20182	CHAIR	M	M.S.E.	ELECTRICAL AND COM	20182			
SANTA MARIA, DANIEL RUIZ	drs2486	20176	CHAIR	M	M.S.E.	ELECTRICAL AND COM	20176			
SAYILAR, GOKHAN	gs23475	20149	MEMBER	M	M.S.E.	ELECTRICAL AND COM	20149			
WANG, YEZHOU	yw4528	20152	MEMBER	D	PH.D.	ELECTRICAL AND COM	20152			
ZHENG, TIANHAO	tz2293	20182	MEMBER	D	PH.D.	ELECTRICAL AND COM	20182			
ZHU, HAISHAN	hz3399	20182	MEMBER	D	PH.D.	ELECTRICAL AND COM	20182			

List of Post-Doctoral Scholars Supervised:

- **Aydin Aysu. Fall 2016 – Summer 2018.**
  - **Co-supervised with Michael Orshansky and Andreas Gerstlauer**
  - **First employment: Tenure-track Assistant Professor, North Carolina State University. Starting Fall 2018.**
  - PhD institution: Virginia Tech
  - PhD advisor: Dr. Patrick Schaumont
  - PhD date: Summer 2016. (July).
  - URL: https://research.ece.ncsu.edu/aaysu/

Budget Council Assessment of Research, Publications & Other Evidence of Scholarship/Creativity
Dr. Mohit Tiwari

Summary

During his tenure as Assistant Professor, Mohit Tiwari has established a stellar research program in secure and trustworthy computer systems, distinguished by its focus on fundamental security vulnerabilities in emerging applications and architectures and the development of mechanisms for their mitigation. Specifically, he has created architectural mechanisms that enable information-leak-free hardware enclaves, containerized data for web services, and anomaly-detection mechanisms. Prior to his arrival at UT, he created oblivious computation mechanisms for a secure processor architecture while working as a postdoctoral researcher at the University of California at Berkeley. At UT, he built upon prior work to solve many of the security challenges and vulnerabilities in current computer hardware and software. He has a very strong record of publication in the highest-quality venues with 14 archival journal/journal-quality conference articles published in rank (29 in career), and has been highly successful in raising substantial extramural funds to support his research. Professor Tiwari's research accomplishments, publication and funding record, and honors make him highly deserving of promotion to Associate Professor with tenure.

Research Area and Contributions

Dr. Tiwari's research is broadly concerned with improving security of emerging computing hardware and software paradigms. The proliferation of social and cloud computing combined with the quest for high performance in the past decades has exacerbated security vulnerabilities in modern computer hardware and software. In recent years, severe vulnerabilities have been exposed in advanced processors including Intel, AMD, and ARM processors. Several of these vulnerabilities are not patchable in existing systems, which leaves essentially all computers today vulnerable to certain attacks and motivates a deep overhaul of the processor design. Software vulnerabilities have been similarly destructive, with compromised data at Facebook and data breaches at Equifax, Target, and Anthem Health proving to be expensive for the companies and harmful for people whose data was breached. It is becoming increasingly clear that patching vulnerabilities as they arise is not a sustainable approach to building computer systems that serve healthcare, elections, and similar sensitive arenas of modern life, and arguably, for any computer system in general.

Tiwari and his group have made critical advances toward fundamentally re-thinking hardware and system software to protect data. His long-term goal is to move computing to a privacy-first model where users own their data while the cloud and applications only provide computing as a utility to the users. His research approach centers around building "enclaves" as a primitive that users can utilize to ensure security of their data. An enclave is a distributed sandbox that enables users' data to be placed inside it such that both the infrastructure (e.g., a cloud or a mobile device) and applications that compute on the data are fully contained within the enclave. A hardware-software system that implements enclaves as a primitive will greatly simplify security by taking it out of the hands of cloud software and applications and associating it directly with the users' data. The challenge is to build enclaves that are indeed secure and private while still providing all the functionality and performance of current systems. Tiwari's research thrust on Software-defined Hardware Enclaves addresses these challenges. A further challenge is to enable large internet-scale services to be run on enclave-based systems. Tiwari's research thrust on Containerized Data addresses this issue. Together, these thrusts are important first steps towards a full-system stack where users work with modern web services while retaining full control over both their data and privacy.

Security is often compromised because emerging economies (such as mobile applications) and new hardware systems (such as sensors or persistent memory technologies) introduce new ways in which systems can be hacked. Hence, in a complementary thrust to enclaved data, Dr. Tiwari has been working on building anomaly detection techniques that detect hardware-level abuses that modern attacks rely on. His work on this theme has informed the design and evaluation of Qualcomm's anomaly detector. He has subsequently collaborated with his colleague at UT ECE, Dr. Shakkottai, on protecting a population of devices, specifically, by encoding system-level insights about attacks into machine learning algorithms. This approach of bringing systems and data-science together results in increased transparency of security alerts and is a stepping stone towards Dr. Tiwari's vision of a semi-autonomous "security plane" for enterprise-scale systems.

Software-Defined Hardware Enclaves

A big challenge in building secure enclaves is that despite encryption and access controls, secret information leaks through what are called side-channels, which can be any software or hardware signature via which attackers use to infer information about the program. Side-channels include various system state, its power draw, or electromagnetic emissions. Side-channels are typically eliminated by modifying the applications or the hardware to normalize algorithm execution or add noise to the execution trace. One major limitation of prior work is that it almost exclusively focuses on protecting cryptographic programs and uses algorithm-specific techniques to prevent the disclosure of cryptographic keys. These techniques are not directly applicable for protecting data inside generic programs, such as those used for data mining and machine learning on private data. Another major limitation is that prior work defends each vulnerability as it is discovered, leaving defenders with many solutions that are tricky to put together into a complete defense. In fact, a solution to one vulnerability can often end up weakening defenses deployed to protect other vulnerabilities.

Dr. Tiwari's research has defined *principled defenses that can close a broad class of side channels* for arbitrary programs. One technique used by Dr. Tiwari relies on the insight that information leakage arises from a program's behavior (i.e., its control- and data-flow) and its subsequent effects on the hardware. He proposed *decoy execution* as a way to close digital side channels that leak secret-dependent variations in program execution. In decoy execution, the program takes paths not taken by the current data so that the adversary sees paths that are independent of the actual secret data. Tiwari's research demonstrated that decoy paths can be made to run correctly and securely. Decoy paths will detrimentally affect program speed and some of Tiwari's research focuses on mitigating the performance effects of decoy execution. This work was published in the top-tier USENIX Security Symposium 2015 and 2016 and demonstrates how to design enclaves with very little changes to existing hardware architectures.

For situations where re-configurable hardware is available (for example, in Microsoft and Amazon cloud services that deploy FPGA processors), Tiwari's research proposes a new microarchitecture with an oblivious memory controller to enable truly-private data storage and an FPGA co-processor to accelerate it. This design places the reconfigurable hardware at the center of security. This is highly advantageous since the reconfigurable hardware can be designed to be trustworthy and isolated from vulnerabilities in the host Intel/ARM processors. When the processor itself can be re-designed, Tiwari identified shared resources such as memory controllers as the channels through which information leaks and proposed efficient ways to partition them to prevent contention with an attacker program. Tiwari's research thus covers a range of hardware and architectural mechanisms to guard various resources such as processor pipeline and memory units against attackers. This work has been published in the highly-selective conferences, such as, CCS 2013, ASPLOS 2015, MICRO 2015, HPCA 2018. Dr. Tiwari's contributions in this area have been widely recognized. The work on decoy execution won the Best Paper Award at ACM Architectural Support for Programming Languages and Operating Systems (ASPLOS) 2015 conference, a top-tier ACM conference. Dr. Tiwari was invited to deliver a plenary talk at NSF's workshop focused on hardware security. In a further recognition, Intel has initiated funding for Dr. Tiwari to re-think Instruction Set Architecture for security.

Containerized Data for Web Services

The dominant way of using enclaves is to ask developers to place application components into different enclaves. While this step improves security by confining the damage in one part of the application from spreading into another, it requires that each developer be a security expert and have full knowledge of their own web application (that is typically assembled from large pieces of existing code), and also understand their users' privacy policies. Even with all this security work, one mistake in a deeply buried library could lead to large breaches, like what occurred at Equifax.

Dr. Tiwari's data containers for applications project, named DATS, introduced "data-security as a service for web applications" by containerizing data. The idea is that the data is partitioned into small segments, and application instances are orchestrated to be confined to one data segment at a time. Even if an application is malicious, Tiwari's scheme prevents leaking data to unauthorized users/servers and from one data segment to another. The elegant aspect is that users who use services, like Dropbox or Google Drive, will see no changes but continue to create and share folders, but apps will be prevented from leaking data across folders. Similarly, for web-services that use Identity and Access Management services on the cloud, DATS uses the policies defined in these services and automatically enforces them on web-services that access the data they control. Tiwari's research contribution has significant impact in that it frees code developers from implementing security features. This work is a major breakthrough in bringing the long-standing field of information flow control to modern web-services. Prior to DATS, information flow-control research from MIT and Stanford required developers to use academic programming languages, and hence the artifacts have been limited to small plug-ins inside web services. With DATS, entire web services can be run with information flow control with support for databases and web-service languages and frameworks. The data containers work was published at ASPLOS 2018, a top-tier ACM conference. Dr. Tiwari and his students have also been working with commercial enterprises (using a seedling NSF Innovation-Corps grant) to productize a simplified version of DATS.

Anomaly Detection to Enterprise Scales

Attackers gain access by triggering malicious hardware backdoors, by stealing secrets through microarchitectural side-channels, by making malware to stress resources, and through other routes. Malicious programs ("malware") often relies on user and developer errors (and oversights) to gain access to sensitive data via new sensor interfaces and program libraries. In order to place defenses against novel threats, Dr. Tiwari has been working on anomaly detection ranging from hardware-level defenses deployed to each device up to a large population of devices.

One important result of Dr. Tiwari's research in this area is it demonstrates the possibility of malware detection via monitoring microarchitecture usage and computational irregularities. His insight is that modern attacks are becoming increasingly anomalous at the instruction level in order to get around software-level defenses or to abuse corner-case hardware behaviors. In response, he uses contention and computation as a channel to identify malware that tries to steal information or gain control over execution by abusing hardware attributes. A major advantage of hardware-level monitoring is that even if software level defenses are breached and software logs or software-log files are untrustworthy, malware cannot avoid executing instructions to achieve their ends. An enclaved hardware-level detector is thus significantly more trustworthy than software-level detectors.

An innovative aspect of Tiwari's work in hardware-level detection is that he assumes that the malware will adapt to any deployed defense. Thus, the system needs to proactively measure the detector against an evasive malware. He introduced the idea that unlike classifiers in traditional machine learning, malware detectors have to be evaluated in terms of their *operating range* to understand the range of malicious behaviors that they can be relied upon to detect. In practice, this dramatically complicates the evaluation methodology to one that requires realistic replays of real applications on hardware, and that also requires a malware generator whose computation can be synthesized to cover a range of behaviors. His MICRO 2016 paper (and an ISCA 2014 workshop paper) discusses these topics in detail and this work forms the basis of his DARPA grant on building open-source processors with anomaly detection built-in.

Each individual anomaly detector is weak and has a significant number of false positives, especially when operated aggressively to detect previously unknown attacks. Hence, a separate project aims to compose detectors (that are individually weak) in noisy enterprises. The idea here is to latch onto "attack vectors" that enable attackers to spread through a population of devices. These vectors can include emails that include malicious attachments, servers that are routinely visited by people in an enterprise, or hardware devices that are plugged into devices. If malware can potentially spread through a vector, Tiwari and his team propose a way to amplify weak detectors by grouping their outputs based on this vector. They show that aggressively looking for suspicious behaviors along attack vector lines can both improve detection of attacks as they happen, and can be used to filter out false positives in large datasets, such as from Symantec (a large antivirus company). This strategy is also robust against new attacks since attack vectors are relatively stationary (and few) while the attacks themselves change rapidly. This population-level aggregation of hardware-level detectors resets the security foundation for enterprises. As Tiwari's research demonstrates, data enclaves filter system-wide activity into a security service whose output amplifies the effect of anomaly detection.

Publications and Impact

Professor Tiwari has an outstanding publication record, with 28 top-tier publications in highly selective IEEE/ACM/USENIX conferences/journals (14 since joining UT), and 11 peer-reviewed workshop papers (3 since joining UT). In the computer architecture and security fields, the top conferences from IEEE/ACM/USENIX are regarded as superior to journals and hence these fields count these conferences as journal-equivalent. Workshop papers in the architecture field are peer-reviewed and are recognized as equivalent to conference publications. His conference publications are all in top-tier IEEE/ACM/USENIX conferences such as MICRO, ASPLOS, HPCA, CCS, Usenix Security, DATE, and HOST.

Significantly, his papers have received prestigious awards at these top venues. Tiwari's CCS 2013 paper that introduced oblivious memory controllers in hardware was selected as one of the ten best applied security papers from the top security conferences, including Security & Privacy, CCS, and Usenix Security. His follow-up paper on an architecture for oblivious computation received the Best Paper Award at ASPLOS 2015 and was invited for a fast-track publication in the prestigious Transactions of Computer Science journal. Tiwari's work on anomaly detection in hardware received the NSF CAREER award, a Google Research award, and a Qualcomm Faculty award (for transitioning the work published at MICRO 2016 to practice). Tiwari's recent work on enclaves for post-quantum cryptography with Dr. Orshansky and Dr. Gerstlauer was a runner-up for the Best Paper Award at HOST 2018. Tiwari's ASPLOS 2014 paper, describing a language to build secure hardware, was selected by the IEEE Micro Magazine as a Top Pick from 2014 (Honorable Mention) across all architecture conferences.

Prof. Srini Devadas of MIT writes that "[I]n the field of secure architecture, in my opinion, Mohit has done the best work of anyone in his age group (or pre-tenure) over the past several years.... Mohit's work stands out because he builds the "right" kind of systems, where at least the specification of the systems can be proven to have strong security guarantees that are convincing to system security and cryptography researchers alike."

Dr. Mihai Christodorescu, who is a Principal Research Scientist at Visa, writes that "I regard ["GhostRider paper"] as a crucial contribution to the area. … This work opened the floodgates of research into practically minded ORAM schemes, and it is likely the reason why leading technology companies (Visa Inc., included) are deploying or considering such approaches in their products and services. … I see a focus in his work on tackling fundamental challenges and creating core technologies, instead of simply addressing the limitations of todays' trendy technologies. … [He] established himself as a key contributor in several security domains (side channels, ORAM, intrusion detection, privacy architectures). I addition, I would like to add that I appreciate his focus on building secure systems, which are both more meaningful and more relevant to the industry, instead of limiting himself to (popular) security attacks. … [He] is an exceptional researcher … with significant potential for future scientific advances."

Prof. Andrew Myers of Cornell University writes that "Dr. Tiwari has been at the center of [security analysis using information flow concepts]. …we can expect his work to have a lasting and recognized impact on computer security. … Dr. Tiwari is probably the top faculty member of his approximate academic age at the increasingly important hardware/security boundary."

Prof. Scott Mahlke of the University of Michigan writes that "[Dr. Tiwari] has become one of the most respected and a true leader in the area of [side channels]. His research record is impressive with a long list of top-tier conference publications in the area of computer architecture and security."

Research Funding

Dr. Tiwari has a stellar record in garnering extramural funds in support of his research. In total, he has received funding for 15 projects totaling approximately $5 million, with his share being approximately $3.5 million. His funding record includes the highly competitive and prestigious NSF CAREER Award, DARPA grants, Google award, Qualcomm Faculty award, Samsung, Huawei, etc. His research is equally valued by federal funding agencies and industry. This level of funding has enabled Tiwari to support projects in a variety of critical areas and to conduct innovative research relevant to the government and industry.

Peer Comparisons

Prof. Tiwari has a strong record of research accomplishment, recognition, and citation impact relative to other researchers at his career stage. The chart below shows a summary of current institution, date of tenure as Associate Professor, year of PhD, Journal/journal quality publications, citations from Google Scholar, and h-index for several leading researchers in the computer architecture/security areas within the past few years (2013-2018). Tiwari is proposed for promotion effective Fall 2019. As shown in the chart, Tiwari compares very well with other top researchers in terms of the number of publications in top venues and the number of high-impact papers (as judged by his h-index) and the number of various awards received. The raw number of citations shows significant variation among the top researchers and is a function of their research subarea, for example, researchers working in artificial intelligence/machine learning related areas tend to get a very high number of citations.

Name/Area	Institution	Title	Dates (PhD / start of current rank)	Pubs in top venues (in rank)	Cites (Jul 27, 2018)	H-ind. (GS) (7/27 2018)	Honors/Awards (in rank)
Chris Batten/ Arch/VLSI	Cornell	Assoc Prof	2010/16	7	1983	18	3- CAREER, AFOSR+DARPA YFA
Daniel Sanchez/ Arch/Systems	MIT	Assoc Prof	2012/18	15	1673	19	5 - CAREER, Top pick ’16, ’17H,’17H, Best paper’15
Hadi Esmailzadeh/ Arch/Machine Learning	GaTech -> UCSD early tenure	Assoc Prof	2013/18	11	4160	22	6 - AFOSR YFA, Qualcomm FA, Top pick’14,’14H, CACM’14, Best paper’16
Mohit Tiwari/ Arch, Security	**UT Austin**	**Asst Prof**	**2011/13**	**12**	**1150**	**18**	**8 - CAREER, Best paper ’15, best paper runner up ’18, Top pick ’15H, Google award 2014, Qualcomm award 2017, Security’13 top-10, TOCS Invitation’15**

Conclusion

Dr. Tiwari is a talented and deeply insightful researcher with innovative contributions into the security of both hardware and software. While in rank, he has made important contributions in hardware and software security. His publications are clear, insightful, and elegantly written and are in top-notch venues. His record of publication in the highest-quality venues is very strong. His talents on both sides of the hardware-software aisle have enabled him to make novel contributions, which many other security researchers who are either on the hardware side or the software side have not been unable to. His research contributions have been recognized through a number of awards. His research area is becoming increasingly relevant each day with the pervasive nature of social media and cloud computing, and the prevalence of security breaches. His record in securing funding for his research from a variety of sources is stellar. His accomplishments in research clearly warrant promotion to Associate Professor position with tenure.

Basis for Evaluation

This Budget Council assessment of Professor Tiwari's research is based on a thorough evaluation of the materials assembled by the candidate for promotion to Associate professor with tenure, in-depth knowledge of the candidate's activities, publications, and research area, and a peer group comparison with researchers at leading institutions.

Prepared by Electrical and Computer Engineering Budget Council Members

Lizy Michael Orshansky

Lizy Kurian John and Michael Orshansky 31 July 2018

5 Significant Publications in Rank

(Students & post-docs supervised by Tiwari are shown in italic)

1. Martin Maas, Eric Love, Emil Stefanov, **Mohit Tiwari**, Elaine Shi, Krste Asanović, John Kubiatowicz, Dawn Song, "PHANTOM: Practical Oblivious Computation in a Secure Processor", *Proceedings of the ACM Conference on Computer and Communications Security* (CCS), pp. 311-324, November 2013, Berlin, Germany. (NYU-CSAW Best Applied Security Paper of the Year, top-10.) https://doi.org/10.1145/2508859.2516692

2. *Casen Hunger, Mikhail Kazdagli*, Ankit Rawat, Alex Dimakis, Sriram Vishwanath, **Mohit Tiwari**, "Understanding Contention-driven Covert Channels and Using Them for Defense", *Proceedings of the International Symposium on High Performance Computer Architecture* (HPCA), pp. 87-101, February 2015, San Francisco, CA. https://doi.org/10.1109/HPCA.2015.7056069

3. *Ashay Rane*, Calvin Lin, **Mohit Tiwari**, "Raccoon: Closing Digital Side-Channels through Obfuscated Execution," *Proceedings of the 24th USENIX Security Symposium*, pp. 431-446, August 2015, Washington, D.C. https://www.usenix.org/node/190909

4. *Mikhail Kazdagli*, Vijay Janapa Reddi, **Mohit Tiwari**, "Quantifying and Improving the Efficiency of Hardware-based Mobile Malware Detectors," *Proceedings of the 49th International Symposium on Microarchitecture* (MICRO), pp. 1-13, October 2016, Taipei, Taiwan. (Transitioned to Qualcomm Malware Research team, led to Qualcomm Faculty Award 2017.) https://doi.org/10.1109/MICRO.2016.7783740

5. *Casen Hunger, Lluis Vilanova**, Charalampos Papamanthou, Yoav Etsion, **Mohit Tiwari**, "DATS: Data Containers for Web Applications," *Proceedings of Architectural Support for Programming Languages and Operating Systems* (ASPLOS), pp. 722-736, March 2018, Williamsburg, VA. https://doi.org/10.1145/3173162.3173213

**Lluis Vilanova worked on this paper as a visitor in my lab in Fall 2014.*

Mohit Tiwari **Research Statement** June 2018

1 Overview

My goal is to construct secure and trustworthy computer systems. Several recent incidents have exposed the deep flaws in today's systems. Users of Facebook had their personal data shared indiscriminately and without their consent through Facebook applications. A small error in an application library led to the Equifax data breach that put 200 million users' financial and identity data in criminal hands. Processor manufacturers found that high-performance features built over the last two decades subtly subvert all software security mechanisms. These three seemingly unrelated debacles are symptoms of an *application-centric security* paradigm—where every application is a trusted steward of user data and implements extremely tricky security techniques on systems that may be actively subverting security.

Vision. My research pursues a radically different *data-centric security* paradigm where users own their data and always control access to it even as the data is created inside untrusted applications and used across mobile and cloud services. Applications merely provide computational utility and cannot affect who can access the data or how it is protected and audited. This data-centric vision will put users and enterprises back in control over their data with help from a few security experts (e.g., the security team at an enterprise) whose decisions can be carefully audited. At the same time, data-centric security will free developers from having to work with security techniques—like authorization and access control, code analysis, application-layer firewalls, and behavioral monitoring—and open up new domains with extremely personal data that are currently inaccessible behind regulatory hurdles.

Research Directions. We are pursuing three research directions to embed data-centric security in a distributed computing stack. First, we need new security mechanisms—information-leak-free enclaves—that can run programs without leaving a trail of metadata clues that an attacker can observe to reconstruct the data. Designing leak-free enclaves when both the program inside the container and the platform services outside are untrusted is an especially challenging problem, since the two can communicate covertly to leak secrets through a myriad of stealthy channels. Section 2 describes **software-defined hardware enclaves** that offer composable, efficient primitives using a combination of hardware and compilers. Second, data-centric security requires a new programming model that enables applications to run in user-owned **data containers**—the key challenge is to enable feature-rich applications to run with high performance. Section 3 describes how we adapt the popular Model-View-Controller programming model familiar to security-novices while our language and operating system techniques automatically import large and diverse applications into our hardware-based data containers. Finally, we observe that threat models and systems components evolve constantly to spawn new attacks—hence, Section 4 details an **anomaly detector** that works at micro-second timescales in hardware and aggregates anomalies as attacks propagate across a graph of millions of machines. Data-centric systems provide anomaly detectors with a cleaner signal (free of application activity) and forces attackers into statistical attacks to escape enclaves—thus, these approaches compose well with each other and greatly amplify the effectiveness of a small security-team.

Current Status. My research group has made significant progress in each direction. Our work on software-defined hardware enclaves defends security-critical post-quantum cryptographic primitives, graph analytics, and database programs, and has received top papers of the year [1, 2] and best paper awards [3, 4] in both computer systems and security conferences. The data container project [5] received an NSF I-Corps grant to help find a market, and is being adopted by cloud-providers like CenturyLink and by financial enterprises to prevent Equifax-like data breaches. Finally, our anomaly detection research [6, 7, 8] can pre-emptively detect a diverse class of processor- and memory-based attacks that have recently garnered significant doomsday-press. This work received an NSF CAREER and a Qualcomm Faculty award and forms the core of our open-source secure-processor research through a DARPA SSITH-program grant.

Future Directions. I plan to build a *semi-autonomous security-plane for enterprise-systems.* In the short term, we will design instruction-set extensions, hardware accelerators, and compilers that enable users and security-experts to synthesize high-level security policies onto each device and coordinate them across a graph of devices using a distributed security service. Longer term, since data-centric systems separate applications from security, we can layer in *active* policies beyond access control and threat detection—specifically, an enterprise-system can proactively set up data containers to be resilient to many failure modes, and use anomalies not as a detector but as a predictor to autonomously respond and adapt to attacks. By considering the attack life-cycle at the enterprise scale and using systems cohesively with machine learning, a small team of security experts can helm large systems that meet enterprise objectives even under attack.

2 Software-defined Hardware Enclaves

Programs spill secrets. Even if data is encrypted and access is controlled, secret information can be inferred through various *side-channels*, which are mechanisms for observing a program's digital footprints through the operating system or hardware architecture, or physical ones such as power draw and electromagnetic emissions. Side-channel attacks have compromised encryption algorithms like AES, RSA, El Gamal, and the Diffie-Hellman key exchange, as well as general purpose applications—for example, our prior work infers secrets from database queries [1] and covertly transmits data across virtual machines at over 500 Kilo bits per second [9] (far higher than the 1 bit per second threshold mandated for high assurance systems). Confining programs that use secret data is the very foundation of a secure cyber-infrastructure—side-channel attacks sabotage confinement.

Side-channels are exceptionally hard to seal. Over the past five decades, numerous solutions have been proposed to defend against side-channel attacks, such as modifying the applications, compilers, operating systems, micro-architecture, and even the gate-level logic family to normalize or add noise to programs' side-effects. These defenses are point solutions that do not compose securely—one defense can *break* others' security guarantees. For example, secure caches that partition caches or randomize the mapping between memory addresses and cache lines break memory trace obliviousness against off-chip adversaries. Further, techniques such as key blinding and metrics that limit information leaks to a few bits per second apply to cryptographic programs and not to a broader class of programs such as machine learning, graph algorithms, database queries, etc.

Our goal is to define principled defenses that can efficiently close a broad class of side channels for the above programs. Specifically, we target *digital* side channels, which are side channels that carry information over bits and digital logic in the system. Digital side channels cover the vast majority of side-channel attacks that use OS, instruction set, or micro-architecture based channels to break encryption and virtual machine isolation. Analog channels such as power draw or electromagnetic radiation typically require physical access to attack and physical measures such as dual-rail logic or capacitors to mask information leaks—these techniques are complementary to our work.

Security: decoy execution [10, 11]. Our first key insight is that digital side-channel leaks arise from secret-dependent variations in program execution—to close these channels, we propose to execute *decoy execution* that take the program's control flows along paths not taken by the current input and create data flows that obfuscates secret values. Intuitively, decoy executions provably create all secret-dependent side-effects so that after obfuscation, an adversary observing *any* digital side-channel sees a trace that is independent of the current secret input. Decoy paths are challenging to run correctly (without crashes and exceptions), securely (controlling hardware side-effects using only architectural registers as trusted memory), and efficiently (without exponentially increasing the number of extraneous control- and data-flow instructions). Our initial work [10] shows that decoy paths are indeed feasible to run correctly and securely—we consider this design as a foundation that fixes the root cause of digital side channels. We then significantly improve the performance of compiler-driven obfuscation and mitigate leaks through floating point computation with sub-normal operands [11]. With over 10× slowdown over native non-secure execution (but almost 10× faster than the closest prior work), our second critical task is to tune performance without breaking security.

Performance: customizable micro-architecture [1, 3, 12, 13]. The security guarantees of compiler techniques as well as performance optimizations require that programs have control over micro-architectural side-effects that attackers can observe. While the baseline decoy path design assumes only architectural registers to be under explicit software control, we propose a new micro-architecture where software can use an oblivious memory controller to index into secret arrays [1] and proposed to instantiate it on an FPGA co-processor to both accelerate it and isolate it from processor vulnerabilities. The subsequent popularity of FPGA servers to accelerate search and machine learning, as well as egregious vulnerabilities in Intel/AMD/ARM CPUs, suggest that our FPGA-based oblivious memory controller is a safer deployment path for computation on sensitive datasets. Beyond memory controllers, the main CPU pipeline itself can be customized by either *partitioning* shared units like memory controllers to prevent contention with an attacker program [12], *shaping* the utilization of attacker-visible resources such as page-accesses, and more broadly exposing control over micro-architectural timing to software [3]. These works lean primarily towards hardware support whereas the decoy executions rely only on architectural registers and `cmovz` instruction for security—one of our primary goals is to define an **oblivious instruction set** that separates users' security requirements from concrete implementations against different threat models.

Metrics: Side-channel privacy. The broad class of programs we target, like machine learning, graph algorithms, and databases, cannot use traditional metrics like bits per second to measure the effectiveness of a defense. The bits per second metric applies to secret keys since keys are random bit sequences, whereas program inputs rarely follow a uniform distribution and leaking a few bits might be sufficient to leak a medical or financial secret in an otherwise large dataset. Worse, program inputs are strongly correlated with a diverse range of side-effects and perfectly normalizing all side-effects will impose extravagant overheads for programs such as database queries or graph analytics. In current work (under submission), we propose *side-channel privacy* as a new metric for micro-architectural side-channels—i.e., to shape side-channel traces such that the side-effect of the current secret input is concealed among that of a large set of inputs. Side-channel privacy has lower overheads than normalizing each execution to produce the worst case trace, and yet retains quantifiable security guarantees through a novel method of applying differential privacy to time series data.

Our work on software-defined hardware enclaves is the first **composable** defense against digital side channels. In contrast, prior defenses have broadly pursued two disjoint fields—information flow control and memory trace obliviousness—along with a host of point solutions that are non-trivial to compose securely. The decoy path approach strives for completeness first, using compilers to carefully normalize all control- and data-flow related side-effects of secret data. But generically obfuscating digital side channels—by normalizing all behaviors or using oblivious memory accesses—is expensive, so we **customize** both the micro-architecture and the security policy to a given program and its side-channel traces across inputs. We propose micro-architecture mechanisms—oblivious memory controllers and private-queues—that programs can use to customize hardware utilization to program-phases. Interestingly, we show that program-phase specific customization can be achieved while concealing the current secret input in the 'crowd' of all possible program inputs (i.e., guarantee side-channel privacy instead of strict isolation). Overall, our compiler analyses and configurable micro-architecture units can enable efficient side-channel freedom for a broad class of programs.

3 Data-containers for Web Services

Data breaches are expensive—a single breach has cost companies like Anthem Health, Target, and Equifax over 100M dollars each. As enterprises move towards using untrusted software as a service across mobile and cloud machines, sensitive data is exposed to breaches through large-scale web-services. In healthcare, especially, the loss of sensitive medical history is irrevocable. Financially, insurance agencies like Lloyd's have suggested that cyber risks are "unusually systemic", unlike natural disasters that affect specific regions, and are potentially too big to cover. Our goal with data-centric security is to eradicate data breaches through web-services.

Breaches occur because data is vulnerable when in use by applications. For example, a healthcare messaging application ("app") has to view and execute queries on clear-text data. If exploited, the application can legally access the entire database and exfiltrate sensitive medical records to an unauthorized user over an HTTPS channel that cannot be firewalled at the network layer. Regulating access control processes through HIPAA compliance or encrypting data at rest and in transit do not address such breaches through compromised apps. Instead enterprises rely on a complicated tangle of partial code-analysis tools during development, and web-application firewalls, patching tools, and machine learning based log analysis during deployment to protect data in use.

Our project—DATS [5]—introduces data-security as a service for web-applications. Our key insight is that, instead of protecting data tangentially by protecting applications, to protect data explicitly by using access control rules to segment the database into small segments, and orchestrating application instances to be confined to one data segment at a time. DATS effectively takes users' access control policies and automatically translates them into information flow control policies on untrusted apps. As a result, even if an app is malicious or compromised it cannot leak data to an unauthorized user or remote server.

Traditional research approaches to information flow control (IFC) are extremely hard to program for and also introduce major performance overheads. Instead, we address the programmability challenge by presenting a security-agnostic application design pattern to developers while transparently implementing novel **robust declassifiers** to safely place data from different data containers in the same storage service or user-facing view. Furthermore, we present **data containers**—operating system containers orchestrated to run fast in a data-centric security system. Data containers can optionally use hardware-capability based fine-grained confinement techniques to further bring down worst case performance overheads.

DATS frees developers from implementing security features and allows them to focus on compelling functionality only. Applications written in popular model-view-controller frameworks can almost directly be ported to efficiently run on DATS. Developers need not be security experts.

For enterprises that use Dropbox or Google Drive, or use Identity and Access Management systems that store access control rules, application users will see no changes. Users continue to create and share folders but with the additional guarantee that apps cannot leak data across folders or outside the system. DATS thus frees enterprises from vetting each application they entrust with sensitive data—this could unleash many creative apps for users and enterprises that today do not have access to sensitive data.

In summary, DATS's support for feature-rich, performant web-services could enable data-centric security to become the default paradigm that reestablishes users' control over their data and privacy. Hence we have undertaken the NSF I-Corps program to find a product-market fit, and have spent over an year piloting prototypes with CenturyLink, MongoDB, and other cloud-providers and enterprises.

4 Anomaly Detection from Hardware to Enterprise Scales

Access to private data makes applications (and even our DATS platform) a prime target for malicious applications (or "malware"), and deep technical problems have to be solved before DATS and application-services become trustworthy. In particular, existing hardware architectures form porous foundations that allow attackers to gain administrator privileges (by hammering rows in DRAM or triggering malicious hardware backdoors, for example), that abets attackers in stealing secrets through micro-architectural side-channels, and that can force missed deadlines. Applications' and DATS' mobile components introduce an additional challenge. While several OS techniques rely on discovering exploits, mobile malware does not use exploits. Instead, malware preys on user errors and new sensor interfaces to access sensitive data, on developer errors in (one of many) program libraries to execute malware with a trusted application's privileges, or it can even succeed by using the user's device only as a networked machine. Without exploits to detect, existing anti-viruses, OS-level techniques, and program analyses fail to detect a large fraction of modern malware.

We observe that, while seemingly disparate, both hardware-level attacks and mobile malware have a common feature—they rely on hiding their hardware-level computation from operating system (OS) level monitors. Hypervisors and operating systems do not monitor micro-architecture usage for side-channel leaks, while mobile operating systems do not track computational irregularities in applications. This observation opens up a new opportunity for defense—**expose hardware computational signals such as programs' instruction-set and micro-architecture behavior to analysis**. We propose to use this computational information to formally study the use of hardware structures as communication channels, and specifically, to model malicious behavior as interference in these hardware channels.

Hardware computational signals come with unique opportunities and challenges. On the one hand, hardware computational signals promise a smaller trusted code base and access to ground-truth information even if the OS is compromised or the malware is stealthy. On the other hand, semantic information about programs may be harder to reconstruct at the hardware level and a malware analysis tool risks being drowned in false positives and false negatives. Our goal is to handle these challenges even when an intelligent adversary is actively trying to evade our analysis. Towards this end, our analysis of hardware channels comprises of the following specific directions:

Contention as a channel [9]. We begin by quantifying the unexplored capacity of covert channels which rely on contention for shared hardware. By separating synchronization from transmission, and explicitly spending a one-time effort to synchronize precisely at the beginning, we demonstrate up to 1 Mbps capacities that are 10–5,000× larger than reported in prior work. However, contending for hardware resources make the attacker observable to a defense that monitors instruction-set and micro-architectural statistics. In response, we show that an attacker can hide behind OS and hypervisor noise to evade detection. To counter such intelligent attackers, we propose a novel detector that deliberately introduces noise to mimic a real application (and thus stays hidden from the intelligent attacker) and yet monitors hardware statistics to classify executions into malicious vs. benign. This research thrust quantified detection results for side-channel detection games in contention-driven hardware channels.

Computation as a channel [6, 7]. We next apply hardware signals to model benign program computation and thus detect mobile malware as computational anomalies. To accurately model an intelligent adversary, we construct a taxonomy of mobile malware behaviors and build a malware analysis platform comprised of both existing and systematically diversified (synthetic) mobile malware. Further, we enable realistic, reproducible experiments by selecting a set of computationally diverse benign applications and build tools to record-and-replay over 1 hour of real human usage for each benign and malware application. Our initial results in detecting malware as a computational anomaly are promising, and show that (a) relatively small software-level malware actions (such as stealing an SMS or a photo) are measurably anomalous compared to a benign program's hardware signature—intelligent malware will have to dramatically slow down its execution to avoid detection, and (b) hardware analysis complements static program analysis—techniques to hide from static program analyses make the malwares' hardware executions more anomalous. These results are surprising given the lack of semantic information at the hardware level, and open up new research into transparent hardware-based malware detector.

4.1 Composing Weak Detectors in Noisy Enterprises

Behavioral detectors do not compose well. This is because malware operates at extremely diverse time- and system-scales to evade detection. For example, malware bypasses network firewalls and packet inspections by luring employees to execute an email attachment (phishing attack) or to visit a URL (waterhole attack) that runs malicious exploits on the employee's machine. The associated timescales are diverse—malware campaigns to lure users through such phishing and waterhole attacks can last for hours to several days and involve thousands of devices. At the other extreme, malware exploits such as JIT-ROP or DRAM RowHammer break operating system level defenses on a single machine to gain super-user privileges within micro-seconds to a few seconds. Composing a single global detector from network, OS, and hardware levels is difficult because the attacks have such diversity of scale.

We propose a scalable paradigm to detect malware in precisely such noisy and transient settings (preprint [8]). Our key observation is that attack patterns induce transient correlations across time and nodes (users). The naive approach of ignoring the low-dimensional structure induced by these transient communities, and simply throwing all alert logs into a "global" classifier can lead to excessive false positives, and any 'signal' will be drowned out by noise in the firehose of alert logs. Thus, our goal is to automatically analyze and reason from alert logs at scale (100,000 nodes, with tens to hundreds of millions of alerts per day), and from a heterogenous mixture of local detectors (potentially different local detectors across the nodes), and develop an algorithmic and statistical framework to substantially drive down the effective number of alerts to human-processing scales (order of tens to hundreds of alerts per day).

To address this goal, we introduce two ideas. 1. Structural: actions such as visiting a website (waterhole attack) by nodes correlate well with malware spread, and create dynamic neighborhoods of nodes that were exposed to the same attack vector. However, neighborhood sizes vary unpredictably and require aggregating an unpredictable number of local detectors' outputs into a global alert. 2. Statistical: feature vectors corresponding to true and false positives of local detectors have markedly different conditional distributions—i.e. their shapes differ. The shape of neighborhoods can identify infected neighborhoods without having to estimate neighborhood sizes—on 5 years of Symantec detectors' logs, Shape-GD reduces false positives from ~1M down to ~110K and raises alerts 345 days (on average) before commercial antivirus products; in a waterhole attack simulated using Yahoo web-service logs, Shape-GD detects infected machines when only ~100 of ~550K are compromised.

5 Future Work

My future work includes getting to substantial milestones that others (including commercial processor vendors) can build upon in each of the above three research directions. Concretely, this includes creating different RISC and CISC variants of oblivious instruction sets and applying them to programs from artificial intelligence, block-chain consensus, graph algorithms, databases, and similar programs that work with secret data. Mapping similar applications into data containers will require creating language-level extensions to handle user-facing functionality as well as program analysis and logging to support debugging of data-containerized web-services (without showing developers user data). We are currently working with the UT Chief Information Security Office to apply our enterprise malware detection techniques to an active network, instead of static datasets. This step will pose new challenges in making our algorithms work on limited time-windows of streaming data without (ideally) losing track of malicious anomalies.

Beyond these individual milestones, I aim to compose the three primitives—using leak-free enclaves to run data containers, while backing up data containers with per-host and enterprise-level anomaly detection. Clearly, by removing application level activity from security logs, the machine learning algorithms will get far cleaner, access-control relevant logs. Further, since data containers tie confinement to access control, applications cannot violate users' privacy by making small application-layer actions and instead have to use statistical techniques to overcome OS- and hardware-level isolation. Forcing attackers into statistical attacks and observing their logs more clearly should ideally make malware more anomalous. Finally, we will move towards more proactive defenses where data containers enable setting up a resilient array of containers that can work with anomaly detectors to predict suspicious neighborhoods of containers and activate responses that bolster defenses (at higher performance cost) or migrate computation. Overall, my research's goal is to place effective security controls in the hands of a small team that can defend enterprises from data breaches and malware.

Table 1. Research Summary

Metric	Value
Peer-reviewed journal publications (in rank and total) ***	2+1 / 6+1
Peer-reviewed *(journal-equivalent)* conference proceedings (in rank and total)	12 / 22
Number of journal papers in rank with supervised student(s) and/or post-docs from UT as co-author(s)* ***	1+1
Number of journal papers in rank with supervised student(s) from UT as co-author* ***	1+1
Number of *journal-equivalent conference* papers in rank with supervised student(s) and/or post-docs from UT as co-author(s)*	8
Number of *journal-equivalent conference* papers in rank with supervised student(s) from UT as co-author*	7
Total citations of all publications (career) from ISI Web of Knowledge*****	178
Largest number of citations for a single paper based on work at UT (ISI Web of Knowledge)*****	29
h-index (career) from ISI Web of Knowledge*****	7
Total citations of all publications (career) from Google Scholar *(as of July 1, 2018)*	1119
Largest number of citations for a single paper based on work at UT (Google Scholar)	143
h-index (career) from Google Scholar	18
Total external research funding raised in rank (personal/total for UT)	$3.56M/$5.05M

NOTES:

*** +1: invited paper to Transactions on Computer Science (TOCS) based on ASPLOS'15 Best Paper Award ("Ghostrider: A hardware-software system for memory trace oblivious computation").

***** ISI Web of Knowledge is missing crucial papers (#2 and #8 from Google Scholar ordered by citation count, and likely others); it has far lower citation counts than Google Scholar for the same papers and has a different set of papers when ordered by citation count.

Table 2. Current External Grants and Contracts

Role of Candidate and Co-Investigators	Title	Agency	Project Total	Candidate's Share	Grant Period
PI: Mohit Tiwari	CAREER: Exo-Core: An Architecture to Detect Malware as Computational Anomalies	NSF CAREER	522,000	522,000	2015—2020
PI: Mohit Tiwari	SaTC: CORE: Medium: Guarding Noisy Neighborhoods with Weak Detectors	NSF	1,200,000	400,000	2017—2021
Co-PIs: Sanjay Shakkottai, Constantine Caramanis					
PI: Christine Julien	CSR: Medium: Extensible Distributed Systems Solutions for Community Supported Child-Independent Mobility	NSF	400,000	200,000	2017—2019
Co-PI: Mohit Tiwari					
PI: Mohit Tiwari	Cyber Security Research on Power Models	Lockheed Martin	500,000	166,000	2016—2018
Co-PIs: Michael Orshansky, Andreas Gerstlauer					
PI: Mohit Tiwari	Mobile Data Container	General Dynamics	166,000	166,000	2017—2019
PI: Mohit Tiwari	Ensembles of Moving Target Defenses for Scalable and Composable Hardware Security	DARPA	748,556	748,556	2018—2021
PI: Mohit Tiwari	Fine-Grained Contention Detection and Mitigation	Huawei-CS Systems Lab	124,000	62,000	2018—2019
Co-PI: Mattan Erez					
PI: Mohit Tiwari	PSigns: Power Channels for Malware Detection	Google award	50,000	25,000	gift
Co-PI: Vijay Reddi					
PI Mohit Tiwari	Hardware-based Malware Detection, Faculty award	Qualcomm award	125,000	125,000	gift
PI: Mohit Tiwari	Anomaly Detection for Cloud Radio Access Network	Huawei-WNCG	100,000	30,000	WNCG gift
Co-PIs: Sanjay Shakkottai, Constantine Caramanis					
Total			**3,935,556**	**2,444,556**	

Table 3. External Grants and Contracts Awarded in Rank and Completed

Role of Candidate and Co-Investigators	Title	Agency	Project Total	Candidate's Share	Grant Period
PI: Mohit Tiwari	TWC: Medium: Collaborative Research: DIORE: Digital Insertion and Observation Resistant Execution	NSF	416,000	416,000	2013—2017
PI: Mohit Tiwari	Establishing a Science of Security Research Lablet at The University of Maryland - Human Reasoning about Privacy and Security	NSA	62,726	62,726	2014—2017
PI: Mohit Tiwari	Hardware Introspection Mechanisms for Debugging and Security	Samsung	100,000	100,000	2016—2017
PI: Mohit Tiwari	I-Corps: Trustworthy Cyberspace through Data-security as a Service	NSF	50,000	50,000	2015—2016
PI: Mohit Tiwari	Architectures to Protect Data in Motion	C-FAR Center at University of Michigan	485,000	485,000	2015—2017
TOTAL			**1,113,726**	**1,113,726**	

Table 4. Pending External Grants and Contracts

Role of Candidate and Co-Investigators	Title	Agency	Project Total	Candidate's Share	Grant Period
PI: Mohit Tiwari (UIUC Co-PI: Chris Fletcher)	Intel ISRA: Oblivious Instruction Set Architectures	Intel	300,000	300,000	2018—2021
PI: Mohit Tiwari (UIUC Co-PI: Chris Fletcher)	SaTC: CORE: Small: Collaborative: Oblivious ISAs for Secure and Efficient Enclave Programming	NSF	500,000	250,000	2018—2021
PI: Mohit Tiwari	Mobile Data Containers Year 2	General Dynamics	217,000	217,000	2018—2019
PI: Mohit Tiwari	Cyber Security Research on Power Models	Lockheed Martin	250,000	83,000	2018—2019
Co-PIs: Michael Orshansky, Andreas Gerstlauer					
TOTAL			**1,267,000**	**850,000**	

References

[1] Martin Maas, Eric Love, Emil Stefanov, Mohit Tiwari, Elaine Shi, Krste Asanovic, John Kubiatowicz, and Dawn Song. Phantom: Practical oblivious computation in a secure processor. In *Proceedings of the 2013 ACM SIGSAC Conference on Computer &#38; Communications Security*, CCS '13, pages 311–324, New York, NY, USA, 2013. ACM.

[2] Xun Li, Vineeth Kashyap, Jason K. Oberg, Mohit Tiwari, Vasanth Ram Rajarathinam, Ryan Kastner, Timothy Sherwood, Ben Hardekopf, and Frederic T. Chong. Sapper: A language for hardware-level security policy enforcement. In *Proceedings of the 19th International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS '14, pages 97–112, New York, NY, USA, 2014. ACM.

[3] Chang Liu, Austin Harris, Martin Maas, Michael Hicks, Mohit Tiwari, and Elaine Shi. Ghostrider: A hardware-software system for memory trace oblivious computation. In *Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS '15, pages 87–101, New York, NY, USA, 2015. ACM.

[4] A. Aysu, Y. Tobah, M. Tiwari, A. Gerstlauer, and M. Orshansky. Horizontal side-channel vulnerabilities of post-quantum key exchange protocols. In *2018 Hardware Oriented Security and Trust*, May 2018.

[5] Casen Hunger, Lluis Vilanova, Charalampos Papamanthou, Yoav Etsion, and Mohit Tiwari. Dats - data containers for web applications. In *Proceedings of the Twenty-Third International Conference on Architectural Support for Programming Languages and Operating Systems*, ASPLOS '18, pages 722–736, New York, NY, USA, 2018. ACM.

[6] Mikhail Kazdagli, Ling Huang, Vijay Reddi, and Mohit Tiwari. Morpheus: Benchmarking computational diversity in mobile malware. In *Proceedings of the Third Workshop on Hardware and Architectural Support for Security and Privacy*, HASP '14, pages 3:1–3:8, New York, NY, USA, 2014. ACM.

[7] Mikhail Kazdagli, Vijay Janapa Reddi, and Mohit Tiwari. Quantifying and improving the efficiency of hardware-based mobile malware detectors. In *The 49th Annual IEEE/ACM International Symposium on Microarchitecture*, MICRO-49, pages 37:1–37:13, Piscataway, NJ, USA, 2016. IEEE Press.

[8] Mikhail Kazdagli, Constantine Caramanis, Sanjay Shakkottai, and Mohit Tiwari. The shape of alerts: Detecting malware using distributed detectors by robustly amplifying transient correlations. *CoRR*, abs/1803.00883, 2018.

[9] Casen Hunger, Mikhail Kazdagli, Ankit Rawat, Alex Dimakis, Sriram Vishwanath, and Mohit Tiwari. Understanding contention-based channels and using them for defense. In *2015 IEEE 21st International Symposium on High Performance Computer Architecture (HPCA)*, pages 639–650. IEEE, 2015.

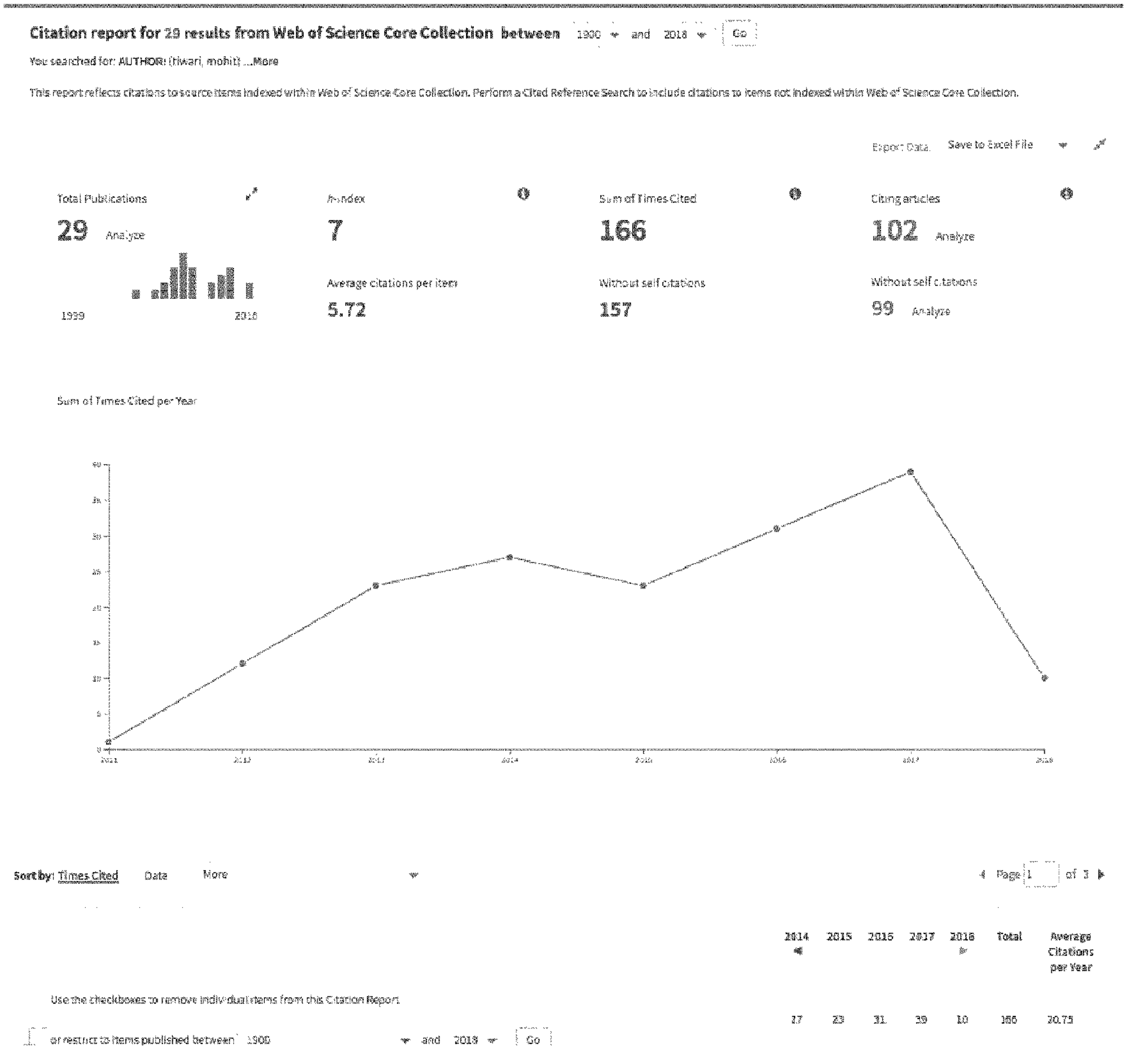
[10] Ashay Rane, Calvin Lin, and Mohit Tiwari. Raccoon: Closing digital side-channels through obfuscated execution. In *24th USENIX Security Symposium (USENIX Security 15)*, pages 431–446, Washington, D.C., 2015. USENIX Association.

[11] Ashay Rane, Calvin Lin, and Mohit Tiwari. Secure, precise, and fast floating-point operations on x86 processors. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 71–86, Austin, TX, 2016. USENIX Association.

[12] Ali Shafiee, Akhila Gundu, Manjunath Shevgoor, Rajeev Balasubramonian, and Mohit Tiwari. Avoiding information leakage in the memory controller with fixed service policies. In *Proceedings of the 48th International Symposium on Microarchitecture*, MICRO-48, pages 89–101, New York, NY, USA, 2015. ACM.

[13] A. Shafiee, R. Balasubramonian, M. Tiwari, and F. Li. Secure dimm: Moving oram primitives closer to memory. In *2018 IEEE International Symposium on High Performance Computer Architecture (HPCA)*, volume 00, pages 428–440, Feb 2018.

Both screenshots dated July 29, 2018.



Citation report for 29 results from Web of Science Core Collection between 1900 and 2018 Go

You searched for: **AUTHOR:** (tiwari, mohit) ...More

This report reflects citations to source items indexed within Web of Science Core Collection. Perform a Cited Reference Search to include citations to items not indexed within Web of Science Core Collection.

Export Data: Save to Excel File

Total Publications
29 Analyze
1999 2018

h-index
7

Average citations per item
5.72

Sum of Times Cited
166

Without self citations
157

Citing articles
102 Analyze

Without self citations
99 Analyze

Sum of Times Cited per Year

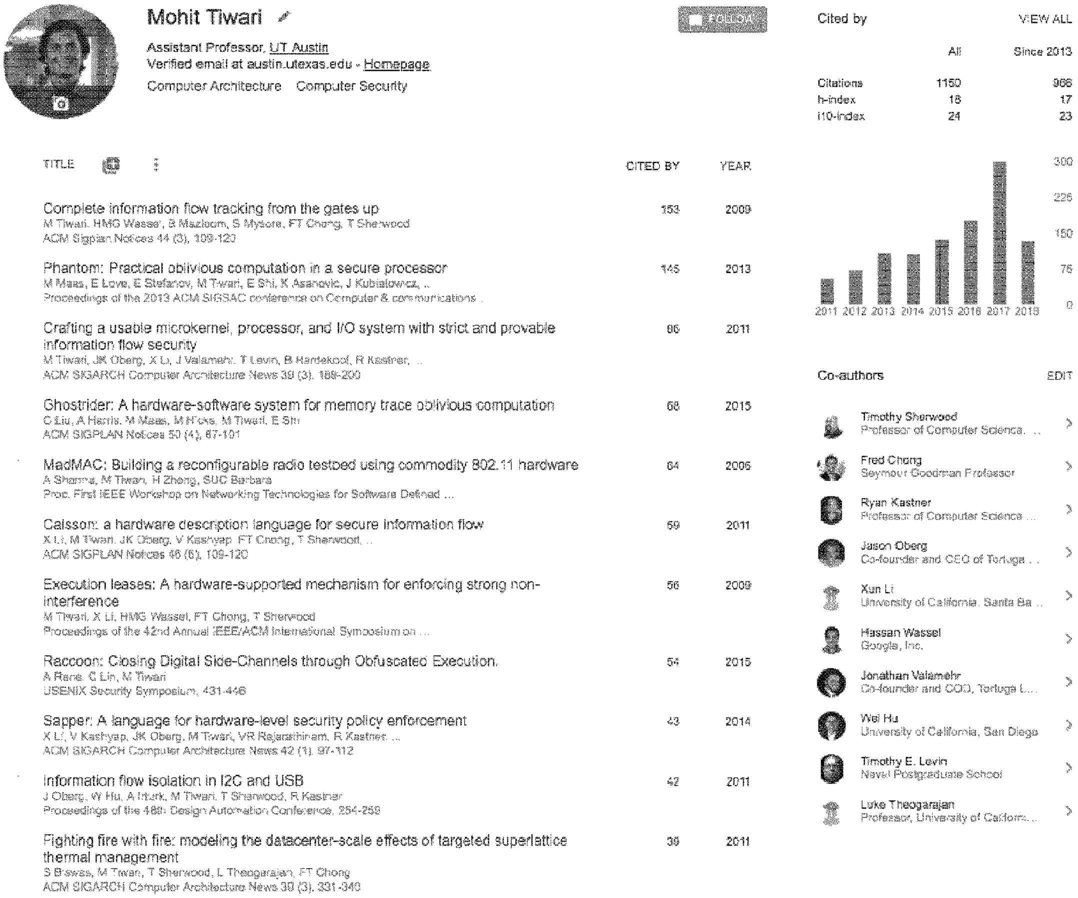
Sort by: Times Cited Date More

Page 1 of 3

Use the checkboxes to remove individual items from this Citation Report

☐ or restrict to items published between 1900 and 2018 Go

2014 ◀	2015	2016	2017	2018 ▶	Total	Average Citations per Year
27	23	31	39	10	166	20.75



Mohit Tiwari

Assistant Professor, UT Austin
Verified email at austin.utexas.edu - Homepage
Computer Architecture Computer Security

TITLE	CITED BY	YEAR
Complete information flow tracking from the gates up M Tiwari, HMG Wassel, B Mazloom, S Mysore, FT Chong, T Sherwood ACM Sigplan Notices 44 (3), 109-120	153	2009
Phantom: Practical oblivious computation in a secure processor M Maas, E Love, E Stefanov, M Tiwari, E Shi, K Asanovic, J Kubiatowicz, .. Proceedings of the 2013 ACM SIGSAC conference on Computer & communications .	145	2013
Crafting a usable microkernel, processor, and I/O system with strict and provable information flow security M Tiwari, JK Oberg, X Li, J Valamehr, T Levin, B Hardekopf, R Kastner, .. ACM SIGARCH Computer Architecture News 39 (3), 189-200	86	2011
Ghostrider: A hardware-software system for memory trace oblivious computation C Liu, A Harris, M Maas, M Hicks, M Tiwari, E Shi ACM SIGPLAN Notices 50 (4), 87-101	68	2015
MadMAC: Building a reconfigurable radio testbed using commodity 802.11 hardware A Sharma, M Tiwari, H Zheng, SUC Barbara Proc. First IEEE Workshop on Networking Technologies for Software Defined ...	64	2006
Caisson: a hardware description language for secure information flow X Li, M Tiwari, JK Oberg, V Kashyap, FT Chong, T Sherwood, .. ACM SIGPLAN Notices 46 (6), 109-120	59	2011
Execution leases: A hardware-supported mechanism for enforcing strong non-interference M Tiwari, X Li, HMG Wassel, FT Chong, T Sherwood Proceedings of the 42nd Annual IEEE/ACM International Symposium on ...	56	2009
Raccoon: Closing Digital Side-Channels through Obfuscated Execution. A Rane, C Lin, M Tiwari USENIX Security Symposium, 431-446	54	2015
Sapper: A language for hardware-level security policy enforcement X Li, V Kashyap, JK Oberg, M Tiwari, VR Rajarathinam, R Kastner, ... ACM SIGARCH Computer Architecture News 42 (1), 97-112	43	2014
Information flow isolation in I2C and USB J Oberg, W Hu, A Irturk, M Tiwari, T Sherwood, R Kastner Proceedings of the 48th Design Automation Conference, 254-259	42	2011
Fighting fire with fire: modeling the datacenter-scale effects of targeted superlattice thermal management S Biswas, M Tiwari, T Sherwood, L Theogarajan, FT Chong ACM SIGARCH Computer Architecture News 39 (3), 331-340	39	2011

Cited by VIEW ALL

	All	Since 2013
Citations	1150	966
h-index	16	17
i10-index	24	23

Co-authors EDIT

Timothy Sherwood	Professor of Computer Science, ..
Fred Chong	Seymour Goodman Professor
Ryan Kastner	Professor of Computer Science ...
Jason Oberg	Co-founder and CEO of Tortuga . .
Xun Li	University of California, Santa Ba ..
Hassan Wassel	Google, Inc.
Jonathan Valamehr	Co-founder and COO, Tortuga L...
Wei Hu	University of California, San Diego
Timothy E. Levin	Naval Postgraduate School
Luke Theogarajan	Professor, University of Californ...

Budget Council Assessment on Advising for the Promotion Candidate Mohit Tiwari

This statement on advising to students by Professor Mohit Tiwari was prepared by the Budget Council Member Professor Vijay K. Garg. It makes an assessment of advising to students performed by Prof. Tiwari in rank as an Assistant Professor.

Graduate Students

Prof. Tiwari has made immense contributions to the Department, the University and the professional community by advising a large number of Ph.D. students. He is currently advising seven Ph.D. students. Of these Ph.D. students, six are being advised as the sole supervisor and one is being advised as a co-supervisor (with Prof. Lin in the CS department). This advising load is well above the average in the ECE department. One student, Mikhail Kazdagli, has finished his Ph.D. dissertation under the supervision of Mohit. He is working at a high-profile startup founded by one of the Android founders. Prof. Tiwari has also graduated three MS students.

Prof. Tiwari also contributes by serving as a mentor for post-doctoral scholars. His mentee, Aydin Aysu, in collaboration with Prof. Orshansky and Prof. Gerstlauer, made fundamental contributions to cryptographic primitives. Aydin is scheduled to start an assistant professor position at NCSU this fall. This level of participation is above average and shows that security is a field with diverse applications and that Prof. Tiwari is willing to help students learn about various techniques in his area.

Undergraduate Students

Prof. Tiwari has supervised five EE 464 Senior Design projects as an assistant professor. These projects require weekly meetings with the group of students and directing the project. Of special note is his supervision of the EE 464H team for the year 2017-2018. This team designed and implemented a IoT Wireless Home Security System. Their project was awarded the best Capstone project award.

Prof. Tiwari has also been an unusually active mentor for undergraduates. His lab has hosted 14 undergraduate students through research positions. These students have gone on to write research papers in international conferences, with one of them winning the best paper nomination. This level of involvement with undergraduates is unprecedented and will go a long way in promoting graduate schools for US citizens.

In summary, Prof. Tiwari has performed advising duties to the graduate students and undergraduate students that is significantly above the level of an Assistant Professor.

Summary prepared by the Budget Council Member Professor Vijay K. Garg.

Vijay Kumar Garg

Academic Advising and Student Placement

Mohit Tiwari
Department of Electrical and Computer Engineering, The University of Texas at Austin
tiwari@austin.utexas.edu

1. Undergraduate Advising

Undergraduate Research. I invest in research opportunities for undergraduates to specifically highlight research as an alternative to the structured workload of courses and industry internships.

From 2013—2018, my lab has hosted 14 undergraduate students primarily through funded summer- and school-year research positions (that pay ~$1,200 and 2,000 per month for year 1/2 and year 3/4 students respectively). I initially recruited these students through talks at UT ECE's IEEE Communication Society meetings and through workshops on computer security. More recently, students who build excellent projects in my undergraduate 319K class apply for an internship at the end of their sophomore or junior year. Almost all students are inexperienced in doing research, hence I pair them with a graduate student and their work involves helping run experiments and read/write paper sections related to live research projects. In addition, the undergraduate students attend group meetings, project-specific meetings, and meet 1:1 with me.

Duration	Names
2014—15 year	Casen Hunger
2015 summer, fall	Manuel Philippose, James Brisson, Joojay Huyn, Domino Rose Weir
2016 summer, fall	Gunalan Karun, Abbas Ally, Anthony Bauer, Kaisheng Song
2017—18 year	Youssef Tobah
2018 summer	Zach Wempe, Steven Zhu, Rahul Butani, Josh Dunning (Rice)

10 of the students have graduated. 4 students, Casen Hunger (UT), Joojay Huyn (UCLA), Domino Weir (GaTech), and Youssef Tobah (UMichigan), have gone to graduate school. Casen joined my lab and has an HPCA'15 first-author paper on his undergraduate research work, while Youssef was a co-author on a HOST'18 Best Paper nominee. Manuel Philippose won a research fellowship from Semiconductor Research Consortium, a UT-level Marjorie Morales award for undergraduate research, and co-authored a PoPETS'18 journal paper, in addition to TA-ing for the Freshman Research Initiative course (described in my teaching statement). Gunalan Karun and Abbas Ally won an award for demonstrating their research at the 2015 Athena Health hackathon.

Capstone Senior Design. I have mentored 5 senior design projects since 2013 comprising a total of 30 undergraduate students. Three of the teams (2014—15, 2015—16, and 2016—17) comprised of students who approached me through my interactions with IEEE Communication Society (CommSoc) and Robotics and Automation Society (RAS) while the other two teams (in 2013—14 and 2016—17) were industry-sponsored projects that both the students (and I) were assigned to.

The first two CommSoc-RAS student projects involved setting up a hardware and simulator for vehicular computer and communication systems. This was an ambitious goal that we found led to technically challenging (and satisfying) work but the senior year timeline made it challenging to finish with a polished prototype. The 2017—18 team thus chose a project they could finish and also have time to polish the prototype. It is extremely satisfying that their strategy and hard work landed them the best Capstone project award.

Duration	Project	Students
2013—14	Acoustic communication channel	Timothy Murray, Rachel Poling, Zachary McDonald, Andrew Studt, Pat Donovan, Mat Geddie
2014—15	Security and Privacy for Intelligent Vehicles	Kevin Gilbert, Gilberto Rodriguez, Christopher Haster, Joshua Bryant, Hao Chen, Young Chou
2015—16	Vehicle-to-vehicle Communication Network Testbed	Miccah Castorina, Kevin George, Omar Medjouri, Arman Mirpour, Nishil Shah, Jimmy Tsao
2016—17	Oil Based Drilling Fluid Characterization for Drilling Hydraulics Optimization Using Data Analytics Techniques	Brian White, Kaisheng Song, Michael Glasser, Scott Fennell, Tong Zhang, Xiaoyong Liang
2017—18	ARM IoT Wireless Home Security System	Weston Hill, Jake Klovenski, Michael Coulter, Ashlie Martinez, Eric Su, Chris Sauceda

2. Graduate and Post-graduate Advising

PhD/MS students. I am currently advising 7 PhD students (1 co-advised with Dr. Calvin Lin in CS) and 1 MS-thesis student, and have graduated 1 PhD, 2 MS-thesis, and 1 MS-with-research students. Mikhail Kazdagli, my first PhD graduate student, started his first position at Essential, a mobile-phone and home-automation startup founded by Andy Rubin (the founder of Android). My MS advisees' first positions were at ARM, Nvidia, and Apple.

Mikhail's work includes applying anomaly detection techniques that he developed for security to debugging and finding root-causes of in-field bugs – these bugs are close to impossible to (re-) create in a test-environment and his unique mix of computer systems and machine learning skills are critical to low-overhead analysis of over 100K mobile devices. For example, his work uncovered the root cause of *jank* (when phone hangs erratically) as stemming from specific finger positions that triggered the fingerprint sensor on the back of the phone. This error manifests as screen lag and unresponsive applications, and cannot be replicated by a few hundred test-users. By placing instrumentation across carefully chosen points in millions of lines of Android code, Mikhail's model was able to trace the anomalous behavior back to the fingerprint sensor software without training on this specific type of bug.

Similarly, Rohith Prakash's job in Apple is specifically to apply our micro-architecture security work on side-channel defenses (discussed in Section 2 of my research statement) to Apple's ARM-based micro-processors.

Post-doctoral Mentees. I have mentored one post-doctoral scholar, Aydin Aysu (2016 PhD, Virginia Tech) in collaboration with Dr. Michael Orshansky and Dr. Andreas Gerstlauer. Aydin worked in the embedded systems security lab that we are bootstrapping in ECE, focusing specifically on securing cryptographic primitives that are resistant to cryptanalysis using quantum computers (hence called *post-quantum or PQ cryptographic primitives*). Aydin's work on PQ decryption and key exchange primitives has been published at top venues (DATE'18 and HOST'18) with a Best Paper runner-up award at HOST'18. He will start a tenure-track Assistant Professor position at North Carolina State University (NCSU) this fall.

Mentoring process. My advising style is customized for each student's personality and their stage of growth. In all cases, as I nudge students towards effective research techniques, I also try very hard to retain the students' core strengths. For example, Mikhail was a sound computer systems engineer and wanted to work in the industry on machine learning related positions. Hence, we picked projects that combined both fields, collaborated with Dr. Ling Huang (Intel) and Dr. Sanjay Shakkottai (UT ECE), and placed him in an industry research lab (Qualcomm Research) where he transitioned his research into products and patents over an extended 8-month internship. My Qualcomm Faculty Award in 2017 is primarily the result of Mikhail's work on improving their hardware-based malware detector. I have followed a similar customized process with other students. Ashay Rane wants to be a professor and has regularly substituted for me in invited talks and taught an FRI course for two years (details in my teaching statement). Casen Hunger is interested in entrepreneurship, hence I have helped him with NSF Innovation Corps and subsequent pilots and fund-raising. Austin Harris is perhaps the most rewarding case: following four years of failed projects, he has found a thesis topic and is additionally the engine behind the extended Univ. of Michigan and Princeton team working on our joint DARPA project.

Beyond this, my lab employs the standard process of meetings for weekly updates, project deep-dives, and 1:1 discussions, and the lab comprises of funded research (and occasionally teaching) assistants and post-doctoral scholars.

Table 1. Summary of Academic Advising

Metric	Value
Student organizations advised	0
Undergraduate researchers supervised***	13 + 1
PhD students completed *(sole supervisions and co-supervisions)*	1 / 0
MS students completed *(sole supervisions and co-supervisions)*	3 / 0
PhD students in pipeline *(sole supervisions and co-supervisions as of 8/31/2018)*	6 / 1
MS students in pipeline *(sole supervisions and co-supervisions as of 8/31/2018)*	1 / 0

*** Undergraduate researchers list comprises of 12 funded summer and school-year positions, 2 unfunded students, and +1 is an undergraduate from Rice University.

Table 2. Degrees Conferred to Graduate Students Supervised

Student Name	Co-Supervisor	Degree	Start Date	Graduation Date	Placement
Mikhail Kazdagli		PhD	08/2013	05/2018	Essential, Inc
Daniel Santa Maria		MS	08/2015	05/2017	ARM
Naveena Sankaranarayan		MS	08/2016	05/2018	Nvidia
Rohith Prakash		MS	01/2015	05/2018	Apple

Table 3. Summary of Graduate Students Currently Supervised at UT Austin

Student Name	Co-Supervisor	Degree	Start Date	Date Reached Candidacy	Date Expected to Reach Candidacy	Expected Graduation Date
Austin Harris		MS, PhD	08/2013		Fall 2018	Spring 2019
Ashay Rane	Calvin Lin, CS	PhD	08/2012**	04/2017		Spring 2019
Casen Hunger		PhD	01/2015		Spring 2019	Spring 2020
Shijia Wei		PhD	08/2016		Spring 2019	Spring 2021
Sarbartha Banerjee		MS, PhD	08/2016		Spring 2020	Spring 2022
Willy Vasquez		PhD	08/2017		Spring 2020	Spring 2022
Prateek Sahu		MS, PhD	08/2017		Spring 2020	Spring 2022
Pranav Kumar		MS	08/2017		Spring 2020	Spring 2022

Budget Council Statement on Service to the University and to the Nation, State and Community for Faculty Promotion Candidate Mohit Tiwari

This report was prepared by Budget Council Member Professor Christine Julien and is her evaluation of Dr. Tiwari's service record.

Evaluation Procedure: The evaluation procedure includes reviewing Dr. Tiwari's annual reports and resumes and is coupled with detailed knowledge of Dr. Tiwari's activities. Dr. Tiwari has been involved in service activities across a wide span of domains throughout his career at UT and has made contributions at or above that which is expected of faculty at comparable rank in the Electrical and Computer Engineering Department.

Administrative and Committee Service:

Assistant Professor Mohit Tiwari has contributed in a variety of ways within the ECE department. For his entire career at UT, he has been actively involved in graduate admissions and recruiting, from annually reviewing applications to co-organizing the visit day for newly admitted students. He has also been heavily engaged in faculty recruiting, serving as a member of both the junior faculty hiring committee and the senior faculty hiring committee. In these capacities, his expertise and engagement in the security and architecture areas have been invaluable. Finally, Dr. Tiwari is also actively engaged in curriculum reform efforts, both in the broader context of the department's overall curriculum and in the ongoing creation of a much needed cyber-security curriculum. At the university level, Dr. Tiwari has been working with UT Austin's CISO Cam Beasley to create a cyber-security operations laboratory with the aim of using UT's extensive network as an experimental testbed platform.

Academic and Professionally Related Public Service:

Externally, Dr. Tiwari is an extremely active and respected member of *both* the computer architecture and cyber-security international communities. In these areas, conference publications are the primary mechanisms of dissemination of research, and service to the community in the form of program committee membership is both a recognition of respect from the community and a significant responsibility. Dr. Tiwari has served multiple times on the program committees of top conferences in both areas (e.g., MICRO, ASPLOS, ICR in computer architecture/systems and Oakland, CCS in security and privacy). He has also been a reviewer for multiple high-profile conferences and journals, and he serves as an associate editor for the ACM Transactions on Architecture and Code Optimization.

Beyond these relatively traditional service outlets, Dr. Tiwari is also engaged in public community activities. Through his work with the Freshman Research Initiative, he performs outreach to both undergraduates and high school students; his research lab also supports many undergraduate researchers. Finally, alongside his graduate students, Dr. Tiwari also routinely shares his cybersecurity expertise with the broader community, e.g., through consulting partnerships with Austin area startups and with Dell Children's Hospital.

Comparison to Other Assistant Professors in the Department:
Assistant professors in the Electrical and Computer Engineering Department are highly involved in both internal and external service activities. Even in that company, Dr. Tiwari's service record exceeds what is expected of assistant professors in the ECE department.

Summary:
Dr. Tiwari's service activities exceed expectations for an ECE faculty member of his rank. Furthermore, the activities are well balanced across service to the department and service to the broader research and public communities.

Statement prepared by Budget Council Member Professor Christine Julien

Service to the University and to the Nation, State, and Community

Mohit Tiwari
Department of Electrical and Computer Engineering, The University of Texas at Austin
tiwari@austin.utexas.edu

I have had multiple opportunities to serve the University, Nation, and Community. Below is a summary of my service activities. Further details may be found in my CV.

1. Service to the University

Graduate admissions committee for ACSES/SES tracks. Since Spring 2013 (prior to starting as an Assistant Professor in Fall 2013), I have been actively involved in the admissions committee that makes admission offers to ~25 PhD and ~40 MS applicants from a pool of ~750 applications. I have also coordinated (together with Dr. Vijay Janapa Reddi until his sabbatical in 2017) the ACSES recruiting day where we recruit the admitted students over a 1-2 day long visit.

ECE junior and senior faculty search committees. I have served on faculty recruiting committees every year after my first year at UT—on the junior hiring committee (2014-15 and 2017-18) and the senior hiring committee (2015-17). Beyond the standard tasks of reviewing applications, hosting candidates, and attending committee meetings, I have actively recruited targeted hires and helped convert the opportunities into offers—for example, Matt Fredrikson, Martin Maas, and Ling Ren as junior faculty in computer systems and Hovav Shacham as a senior computer security recruit. Hovav will join UT CS this fall, having chosen CS over ECE, but we will run a cybersecurity program (including courses and seminars) that will be open to both CS and ECE students.

ECE curriculum reform committee. I have been working as part of the curriculum reform committee to make the ECE curriculum more cohesive, whereby concepts from seemingly unrelated domains can be inserted as examples into each class. Furthermore, I have been working with teaching teams of EE 319K and 312 to find more effective ways to co-teach embedded systems (interfacing across digital and analog domains) and programming (writing structured programs). This work is in addition to the cyber-security curriculum development that I am working on together with Dr. Suzanne Barber, Dr. Hovav Shacham, and UT's CISO Cam Beasley.

2. Service to the Community, State, and Nation

NSF Panelist. I have served on various panels for the NSF Secure and Trustworthy Cyberspace (SaTC) program since 2014, reviewing and helping make funding recommendations for academic project proposals.

Cybersecurity advisor to Austin tech-startups and Dell Children's hospital. My students and I help technical startups based in Austin, San Antonio, and the bay area navigate cybersecurity problems. In particular, we have helped startups that deploy web-services in third-party cloud services (including financial, healthcare, and block-chain based services) and have to meet strict compliance requirements (like HIPAA, PCI, etc). We meet these companies primarily through the

Build-Sec Foundry (a cyber-security accelerator run out of Austin and San Antonio), through Capital Factory (a tech-startup accelerator based in downtown Austin), and through mentees of Professor Sriram Vishwanath (who advises several Austin startups from bootstrapping through Series-A fund-raising rounds).

Hosting undergraduates in laboratory and high-school outreach program. I host several undergraduate students from UT Austin and Rice areas in my lab as researchers. I taught the Freshman Research Initiative (FRI) programs where we taught cybersecurity research to ~30 undergraduates. I conducted workshops for undergraduates (in cybersecurity, as part of IEEE CommSoc) and for high school students (as part of FRI recruitment program). My teaching and advising statements describe these in more detail.

3. Service to the Professional Community.

While I am primarily a member of the computer architecture community (i.e., the community around ISCA, MICRO, HPCA, and ASPLOS conferences), I also publish in and help the cyber-security community (that runs IEEE S&P, CCS, Usenix-Security) as well. Please refer to my CV for details.

Program committees. In the last five years, I have served on the program committees of top conferences in both computer architecture and computer security. These include ISCA, MICRO, HPCA, and ASPLOS for computer architecture; S&P and CCS for security; and a third community that overlaps architecture, security, and hardware design-automation (HOST). Beyond these top-tier conferences, I have been on the program committee of niche venues such as CGO, ISPASS, CARL, HASP, etc that focus on topics in architectures, compilation, and workload characterization.

Guest- and Associate-Editor for journals. I was invited to guest-edit the security edition of computer architecture's flagship journal/magazine, IEEE Micro, in September 2016. I am an associate editor for the ACM Transactions of Code Optimization (TACO), the computer architecture focused ACM journal, and edit papers on secure architectures.

Budget Council Assessment of Honors and Other Evidence of Merit or Recognition, Including Contracts and Grants for Promotion Candidate Mohit Tiwari

Prepared by Yale Patt, Budget Council Member

This assessment is based on Dr. Tiwari's statements and CV, augmented by my own impressions of the importance of each accolade, and from information on official websites of several agencies and companies.

It is clear from both the substantial number of accolades he has already been awarded and the significant amount of research funding he has received that Professor Mohit Tiwari is a rising star in the field of Computer Security. I will delineate in turn his most important honors and the most significant examples of his research funding.

Part I. HONORS AND RECOGNITION

a. 2015 NSF CAREER Award

The NSF CAREER Award is the honor essentially all science and engineering young faculty aspire to. Since the early 1980s when it was known as the NSF Presidential Young Investigator Award, it has identified those assistant professors who are expected to be future leaders in their respective fields.

b. 2011-2013 NSF Computing Innovation Post-doctoral Fellowship

After obtaining his PhD at UC Santa Barbara, Dr. Tiwari was awarded a highly competitive NSF post-doc to work with Professor Dawn Song, a leading scholar in Computer Security at UC Berkeley.

c. Best paper awards

Dr. Tiwari has a strong record of publication in top conferences, which includes Best Paper Awards in two of them, one in ASPLOS in 2015, and one in PACT in 2009. He is also a co-author of a recent paper (May, 2018) which was designated Best Paper "runner-up" in the International Symposium on Hardware-Oriented Security and Trust (HOST). As a post-doc at Berkeley, he was part of the team that produced PHANTOM, which was published in the ACM Conference on Computer and Communications Security, November 2013. This paper was selected by NYU as one of the top 10 security papers of the year 2013. Finally, his paper while he was still a graduate student was selected as one of the outstanding research papers of 2009 and published in IEEE Micro's 2010 Top Picks Special Issue.

I note that all these papers are refereed conference papers. Unlike most science and engineering disciplines, computer science and engineering in general and computer architecture in particular has a long tradition of more than 30 years of history in regarding archival conference papers in top conferences as more prestigeous than archival journal papers.

Citations of the papers described above are listed below:

Chang Liu, Austin Harris, Martin Maas, Michael Hicks, Mohit Tiwari, Elaine Shi, "GhostRider: A Hardware-Software Sysem for Memory Trace Oblivious Computation," ASPLOS, March 2015. Best Paper Award.

Mohit Tiwari, Shashidhar Mysore, Timothy Sherwood, "Quantifying the Potential for Program Analysis Peripherals," Sept 2009, PACT. Best Paper Award.

Aydin Aysu, Youssef Tobah, Mohit Tiwari, Andreas Gerstlauer, Michael Orshansky, "Horizontal Side-Channel Vulnerabilities of Post-Quantum key Exhange Protocols, HOST May 2018, Best Paper Award runner-up.

Martin Maas, Eric Love, Emil Stefanov, Mohit Tiwari, Elaine Shi, Krste Asanovic, John Kubiatowicz, Dawn Song, "PHANTOM: Practical Oblivious Computation in a Secure Processor," ACM Conference on Computer and Communications Security, November, 2013.

Mohit Tiwari, Xun Li, Hassan Wassel, Bita Mazloom, Shashidhar Mysore, Frederic Chong, and Timothy Sherwood, "Gate-Level Information-Flow Tracking for Secure Architectures," 2010 IEEE Micro Top Picks,

d. Prestigious Invited Lectures

Dr. Tiwari has already been invited to give two plenary addresses: the Keynote address at the 2016 Workshop on Computer-Aided Design and Implementation for Cryptography and Security (CADICS) at ICCAD, and this year at the NSF workshop on Side- and Covert-Channels Security in Washington, DC. He was also selected in 2017 as one of the 12 "world-class researchers" to teach at the European Union's annual summer school for PhD students, ACACES.

e. Industry Recognition

Two companies, Qualcomm (in 2017) and Google (in 2014), have given Dr. Tiwari Faculty Research Awards. Such awards are generally based on a recognition that the faculty member is doing outstanding, relevant research and is a mechanism a company uses for honoring and encouraging selected researchers.

Part II. FUNDING

Dr. Tiwari has amassed an impressive record of research funding. He has been part of grants and contracts totaling $5,049,282, of which his share is $3,558,282. What is particularly notable about Dr. Tiwari is that he has been successful pursuing research funding by himself, and he has also been successful obtaining research funding as a team player in collaboration with other UT faculty. Listed below are his most significant research grants and contracts.

a. By himself:

NSF CAREER Award, $522,000, 3/15-2/20 "Exo-Core: An Architecture to Detect Malware as Computational Anomalies" "Digital Insertion and Observation Resistant Execution," $416,000 8/13-8/17. NSF Secure and Trustworthy Cyberspace program.

"Architectures to Protect Data in Motion," $485,000, 5/15-12/17. Michigan Center for Future Architectures Research"

"Mobile Data containers," $374,263 6/17-8/19. General Dynamics.

"Ensembles of Moving Target Defenses," $748,556 10/17-1/21. DARPA System Security Integration through Hardware and Firmware Program.

b. In collaboration with colleagues.

"Cybersecurity Research on Power Models," $500,000. Lockheed Martin (with M. Orshansky and A. Gerslauer)

"Guarding Noisy Neighborhoods with Weak Detectors," $1,200,000 (his share, $400,000), 3/17-2/21. NSF Secure and Trustworthy Cyberspace program. (with S. Shakkottai and C. Caramanis),

"Extensible Distributed Systems Solutions for Community Supported Child-independent Mobility," $400,000 (his share $200,000) 9/17-8/19 NSF's Computer Systems Research program. (with C. Julien)

8 August 2018

Honors and other Evidence of Merit of Recognition, Including Contracts & Grants

Mohit Tiwari
Department of Electrical and Computer Engineering, The University of Texas at Austin
tiwari@austin.utexas.edu

1. Awards

My research program at UT has been recognized through awards for both personnel and papers. I have received an NSF CAREER award for my proposal on using hardware-level anomalies to detect malware; and a Qualcomm Faculty Award for transitioning this work into their product (note that this award is nominated internally without my involvement in the application process). I received a Google faculty research award in collaboration with Dr. Janapa Reddi (UT ECE) and was privileged to be a Fellow of the AMD Chair in ECE during 2017-19.

Our paper in CCS'13 was selected as one of the top ten best applied security papers of the year in computer security (i.e., from the papers published at *any* top venue in cyber-security and computer systems in 2013). Its follow-on work at ASPLOS'15 won the Best Paper Award and was invited to a fast-track publication in Transactions on Computer Science (where the editor-in-chief publishes the paper without additional reviews). My ASPLOS'14 paper received an honorable mention from IEEE Micro Top Picks edition, which selects the best of the papers published in *all* computer architecture conferences. My work on post-quantum key exchange security (with Michael Orshansky and Andreas Gerstlauer) was a runner-up in the Best Paper Award competition. This line of work was the focus of our post-doctoral scholar Aydin Aysu's presentation at his job interviews—he will join North Carolina State University this fall as a tenure-track assistant professor.

In addition, a graduate student in my group, Ashay Rane, won a distinguished paper award at Usenix 2017 for an internship project at Microsoft Research (applying our work to verifying hardware-level security properties of their cryptographic library). An undergraduate student, Manuel Philippose, won the UT Marjorie Morales award for undergraduate research and an SRC-fellowship during his senior year.

2. Research Funding

I have secured approximately $5.05M of research funding with my collaborators at UT Austin and outside, of which my research group's share is ~$3.56M. This funding came from diverse sources, including NSF, DARPA, SRC, and companies. My CV and research statement provide further details about funding.

3. Invited, Keynote, and Plenary Talks

I have been invited to be a keynote speaker at the CADICS security workshop (with ICCAD 2016), a teacher at the prestigious ACACES summer school in Fiuggi, Italy (2017), and a plenary speaker at the NSF Workshop on Side- and Covert-channel Security (2018).

Beyond these prestigious talks, I have delivered several invited talks at universities, technical conferences and workshops, and companies. More information on these are in my CV.

3. High Impact Publications.

My research group's results have been published exclusively in high-impact top-tier conferences (that are considered journal-equivalent). These include architecture conferences (MICRO'15, '16), HPCA'15, '18, ASPLOS'14, '15, '18), computer security venues (CCS'13, Usenix Security'15, '16, PETS'18), and hardware-design venues (HOST'18, DATE'18). We initially published at a few workshops (CARL'13, HASP'14a, '14b) but then decided to focus exclusively on top-tier conferences. The papers' impact can be evaluated through awards—for five of the thirteen papers (CCS'13, ASPLOS'14, '15, MICRO'16, and HOST'18)—through technical transfer (MICRO'16), and through commercialization efforts (NSF I-Corps award related to ASPLOS'18).

Mohit Tiwari
LETTERS REQUESTED/RECEIVED

Name of reviewer, rank or title, department, university	David Brooks, Haley Family Professor, Maurice Wilkes award Computer Science Harvard University
Brief statement of expertise and reason for selection	Expert in computer architecture, cross-layer system design
COI	No
Other relevant information	David Brooks was part of a center that Mohit was affiliated with -- there is no conflict since Mohit was invited to be part of this center and didn't write a shared proposal with David. All interactions between Mohit and David have been limited to attending center workshops twice a year from 2015--17, in addition to standard computer architecture and systems conferences. U.S. Dept. of Commerce Silver Medal "For developing a vision, strategy, fit-up, fabrication processes, policies, protocols, and a safety program for the NIST AML Nanofab," 2006, National Institute of Standards and Technology
Nominated by	Department
Date letter received	August 17, 2018

Name of reviewer, rank or title, department, university	Mihai Christodorescu Principal Research Scientist, Security Visa Research
Brief statement of expertise and reason for selection	Expert in computer security, anomaly detection, programming languages
COI	No
Other relevant information	Leader in the area of anomaly detection at both the device and enterprise scales
Nominated by	Candidate
Date letter received	July 30, 2018

Name of reviewer, rank or title, department, university	Srinivas Devadas Edwin S. Webster Professor, IEEE/ACM Fellow Electrical Engineering and Computer Science MIT
Brief statement of expertise and reason for selection	Expert in computer architecture, computer security, applied cryptography
COI	No
Other relevant information	
Nominated by	Candidate
Date letter received	July 20, 2018

Name of reviewer, rank or title, department, university	Chris Kruegel Professor Computer Science Department UC Santa Barbara
Brief statement of expertise and reason for selection	Expert in computer security, enterprise security, malware analysis
COI	No
Other relevant information	H-index of 86, 27K citations, has led the field of malware analysis for enterprise systems in both research and deployment (through his company, Lastline)
Nominated by	Department
Date letter received	August 20, 2018

Name of reviewer, rank or title, department, university	John Kubiatowicz Professor Electrical Engineering and Computer Science UC Berkeley
Brief statement of expertise and reason for selection	Expert in computer architecture, computer security, internet-scale systems Presidential Early Career Award for Scientists and Engineers (PECASE)
COI	Prof. John Kubiatowicz was a co-author on a paper Mohit started in Berkeley; John happened to be a co-advisor to a first-year graduate student on the project and hence had his name added to the paper. This paper does not reflect an actual conflict.
Other relevant information	
Nominated by	Department
Date letter received	August 20, 2018

Name of reviewer, rank or title, department, university	Scott Mahlke Professor and Associate Chair Electrical Engineering and Computer Science Department University of Michigan
Brief statement of expertise and reason for selection	Expert in computer architecture, compilers; specifically, application-specific processors
COI	No
Other relevant information	Scott Mahlke was part of a center that Mohit was affiliated with -- there is no conflict since Mohit was invited to be part of this center and didn't write a shared proposal with Scott. All interactions between Mohit and Scott have been limited to attending center workshops twice a year from 2015--17, in addition to standard computer architecture and systems conferences.
Nominated by	Department
Date letter received	August 2, 2018

Name of reviewer, rank or title, department, university	Onur Mutlu Professor, Department of Computer Science, ETH Zurich Adjunct Professor of Electrical and Computer Engineering, Carnegie Mellon University
Brief statement of expertise and reason for selection	Expert in computer architecture, computer security, computer systems
COI	No
Other relevant information	
Nominated by	Candidate
Date letter received	August 18, 2018

Name of reviewer, rank or title, department, university	Andrew Myers Professor, Computer Science Department Cornell University
Brief statement of expertise and reason for selection	Expert in programming languages, computer security, information flow control in distributed large-scale systems
COI	No
Other relevant information	ACM Fellow
Nominated by	Candidate
Date letter received	August 3, 2018

Name of reviewer, rank or title, department, university	Moinuddin Qureshi Professor, School of Electrical and Computer Engineering Georgia Tech
Brief statement of expertise and reason for selection	Expert in computer architecture, memory systems, computer security
COI	No
Other relevant information	Moin Qureshi was part of a center that Mohit was affiliated with -- there is no conflict since Mohit was invited to be part of this center and didn't write a shared proposal with Moin. All interactions between Mohit and Moin have been limited to attending center workshops twice a year from 2015--17, in addition to standard computer architecture and systems conferences.
Nominated by	Department
Date letter received	August 15, 2018

Name of reviewer, rank or title, department, university	Josep Torrellas Saburo Muroga Professor, Electrical and Computer Engineering University of Illinois at Urbana-Champaign
Brief statement of expertise and reason for selection	Expert in computer architecture, parallel computing, computer security IEEE/ACM Fellow
COI	No
Other relevant information	
Nominated by	Department
Date letter received	August 15, 2018

DEPARTMENT OF ELECTRICAL AND COMPUTER ENGINEERING
Cockrell School of Engineering

Engineering Education & Research Center (EER), 2501 Speedway, Room 2.864, C0803 • Austin, Texas 78712

June 12, 2018

The Department of Electrical and Computer Engineering sincerely appreciates that you have agreed to serve as Formal Reviewer in the University of Texas at Austin's Tenure and Rank Advancement Promotion case of Dr. Mohit Tiwari.

You are being asked to provide a candid assessment in the area of Scholarly Distinction to assist our decision-making process. Specifically, you will be submitting a Letter of Review assessing major engineering and/or scientific contributions.

Instructions:

1. Access candidate materials here: Tiwari Promotion Materials
2. Your Letter of Review should address the following:
   a. Do you know the candidate, and if so, for how long and under what circumstances?
   b. What are the original, innovative, and/or important contributions that the candidate has made in his/her field of research? Have the candidate's publications influenced the thinking of, or the methods used by, others in the field?
   c. How would you assess the candidate's development compared with cohorts in research-intensive universities?
   d. What is your perspective on the candidate's promise for further professional growth and leadership?
   e. We would welcome any additional comments you might have. The more specific you can be in your comments, the more helpful your evaluation will be.

   Please note: Under the laws of the State of Texas, the candidate has the right to view any materials in his/her personnel file, including your letter. Members of our faculty and internal review committees who see your letter as part of the promotion process will hold the comments you make in confidence.
3. Submit the following by end of day July 27, 2018, in order for your assessment to receive full consideration:

   Your signed Letter of Review on institutional letterhead, including the URL for your website containing your short Curriculum Vitae (or an attachment of your short-version CV), via scan to: http://www.ece.utexas.edu/upload

Thank you for your assistance with this important matter. As faculty members, we realize that the amount of time required to do a thoughtful review is considerable.

Sincerely,

Ahmed Tewfik

Dr. Ahmed Tewfik
Cockrell Family Regents Chair in Engineering
Chairman, Department of Electrical and Computer Engineering

MOHIT TIWARI – MATERIALS SENT TO REFEREES

1) Curriculum Vita
2) Teaching Statement
3) Research Statement
4) Five Significant Publications

5 Significant Publications in Rank
(Students & post-docs supervised by Tiwari are shown in italic)

1. Martin Maas, Eric Love, Emil Stefanov, **Mohit Tiwari**, Elaine Shi, Krste Asanović, John Kubiatowicz, Dawn Song, "PHANTOM: Practical Oblivious Computation in a Secure Processor", *Proceedings of the ACM Conference on Computer and Communications Security* (CCS), pp. 311-324, November 2013, Berlin, Germany. (NYU-CSAW Best Applied Security Paper of the Year, top-10.) https://doi.org/10.1145/2508859.2516692

2. *Casen Hunger, Mikhail Kazdagli*, Ankit Rawat, Alex Dimakis, Sriram Vishwanath, **Mohit Tiwari**, "Understanding Contention-driven Covert Channels and Using Them for Defense", *Proceedings of the International Symposium on High Performance Computer Architecture* (HPCA), pp. 87-101, February 2015, San Francisco, CA. https://doi.org/10.1109/HPCA.2015.7056069

3. *Ashay Rane*, Calvin Lin, **Mohit Tiwari**, "Raccoon: Closing Digital Side-Channels through Obfuscated Execution," *Proceedings of the 24th USENIX Security Symposium*, pp. 431-446, August 2015, Washington, D.C. https://www.usenix.org/node/190909

4. *Mikhail Kazdagli*, Vijay Janapa Reddi, **Mohit Tiwari**, "Quantifying and Improving the Efficiency of Hardware-based Mobile Malware Detectors," *Proceedings of the 49th International Symposium on Microarchitecture* (MICRO), pp. 1-13, October 2016, Taipei, Taiwan. (Transitioned to Qualcomm Malware Research team, led to Qualcomm Faculty Award 2017.) https://doi.org/10.1109/MICRO.2016.7783740

5. *Casen Hunger, Lluis Vilanova**, Charalampos Papamanthou, Yoav Etsion, **Mohit Tiwari**, "DATS: Data Containers for Web Applications," *Proceedings of Architectural Support for Programming Languages and Operating Systems* (ASPLOS), pp. 722-736, March 2018, Williamsburg, VA. https://doi.org/10.1145/3173162.3173213

*Lluis Vilanova worked on this paper as a visitor in my lab in Fall 2014.

BC

HARVARD
John A. Paulson
School of Engineering
and Applied Sciences

David M. Brooks
Haley Family Professor
of Computer Science

August 15, 2018

I am responding to a request for evaluation of Dr. Mohit Tiwari's promotion to a tenured faculty position at the University of Texas, Austin. I have not collaborated with Dr. Tiwari on any research projects, but I have been familiar, and quite impressed, with Dr. Tiwari's research since his PhD studies at UC Santa Barbara. His research at UT-Austin continues to focus on the very important area of hardware security and he has established a robust research program in this area. To summarize my opinion, which I elaborate on in the remainder of this letter, I *strongly recommend* that Dr. Tiwari be granted tenure at UT-Austin.

Researchers in computer security have traditionally focused on the software layers. However, over the last several years, computer architecture security research has started to gain significant traction. The Spectre and Meltdown attacks have drawn significant attention to this research area, including tremendous interest in the popular press. The combination of Dr. Tiwari's work in the hardware security area represents a body of research that sets the standard for other computer architects. While computer architects have been a bit slow to get into security research, Dr. Tiwari is clearly far ahead in this area, and I expect him to be a leading scholar in this very important subfield for the coming years.

Although I have not specifically focused my research on computer security, I am very impressed by Dr. Tiwari's work in this area. I think it is fair to say that over the past five years, Dr. Tiwari has established himself as one of the top researchers in this sub-field of computer architecture, along with Dr. Ruby Lee from Princeton University, Dr. Ed Suh from Cornell University, and Dr. Simha Sethumadhavan from Columbia University. Dr. Tiwari's security research is both broad and deep -- he has a series of publications on detecting and isolating side-channel vulnerabilities, which seems to be his specialty. At the same time, he has moved into new areas like mobile malware detection and data containers for cloud computing environments.

In preparing this letter, I studied the five significant publications that were provides as part of Dr. Tiwari's dossier. These papers really emphasis the breadth and depth of Dr. Tiwari's research. In particular, I really enjoyed reading the work at the USENIX Security Symposium in 2015 titled "Raccoon: Closing Digital Side-Channels through Obfuscated Execution." This work sketches out the different avenues for attack in a typical system and sets out a program source-code level approach to obfuscating the true execution pattern by creating the illusion that multiple program paths are being executed. The paper describes a full system demonstrating the approach and provides a detailed comparison with Dr. Tiwari's earlier work, called Ghostrider.

Dr. Tiwari's research trajectory over the past several years has been quite good as he ramps up his research program. Dr. Tiwari has published several papers in top-tier computer architecture conferences, including HPCA in 2018, ASPLOS in 2018 and 2015, and MICRO in 2016 and 2015. In addition, Dr. Tiwari has published in top computer security venues like the USENIX Security Symposium and the IEEE HOST conference. In short, Dr. Tiwari is publishing his work in the top venues for his field of research.

Dr. Tiwari has an excellent track record of attracting funding for his research. Dr. Tiwari's funding base is also quite very diverse with a significant amount from NSF and industry sponsors. Recently, Dr. Tiwari landed a large DARPA grant as part of the SSITH program. It's clear that there is a real hunger for research in this area from both government and industry sponsors. I am not surprised that Dr. Tiwari has been successful in attracting significant research funding, given both the importance of the area and Dr. Tiwari's track record and research accomplishments.

In addition to his technical contributions, Dr. Tiwari has performed a significant amount of service to the research community through program committees, journal reviewing, and conference organizing activities. I do not have special knowledge of Dr. Tiwari's teaching, but from looking through his CV, it appears that he has helped launch a cybersecurity curriculum in UT's ECE department. He has also collaborated with Dr. Lin to develop a freshman research initiative in cybersecurity. These curriculum advances are both impressive accomplishments for a junior faculty member.

In summary, Dr. Tiwari is one of the leading young researchers in the area of computer hardware security. His research output and productivity is commensurate with other recently tenured computer architects, including Dr. David Wentzlaff at Princeton and Dr. Chris Batten at Cornell. In my opinion, Dr. Tiwari clearly meets the standard for promotion to Associate Professor with tenure at any top ECE department. I would be happy to provide any further information about Dr. Tiwari if it may be of help.

Sincerely,

Dr. David Brooks

From: David Brooks <dbrooks@eecs.harvard.edu>
Sent: Friday, August 17, 2018 8:10 PM
To: Erengil, Jac <jac.erengil@utexas.edu>
Subject: Re: Tiwari Promotion Letter

Hi Jac,

I'm sorry for the very slow reply. I've attached my letter to this email, as well as a recent version of my CV. Do I need to upload it somewhere else?

-David

David M. Brooks
Harvard University

- Haley Family Professor of Computer Science
- Area Co-Chair for Electrical Engineering

Professor Brooks' research focuses on the interaction between the architecture and software of computer systems and underlying hardware implementation issues. A major focus of his research has been to explore how lower-level design issues such as power dissipation and chip cooling can be modeled and addressed when making early-stage architectural decisions in computer systems.

Exploring new architectures and software techniques that are aware of energy, temperature, and other lower-level design metrics is extremely important when designing modern computer systems. New emphasis on computer systems that optimize design metrics besides raw performance, such as battery life, form-factor, and cost-efficiency provide many new challenges for system designers. As the underlying technology continues to evolve, new design issues arise and existing challenges become more difficult. In many cases, architectures that are aware of these issues provide superior overall solutions.

Professor Brooks' recent work has focused on linking architectural performance simulators with early stage power and temperature models. The methodology behind this work has been applied to academic research tools such as Wattch. Similar tools have been developed and used within industry, both for research and in early stage owner-analysis of product designs.

C

VISA

July 29, 2018

Mihai Christodorescu
Principal Research Scientist

To the Chairman of the Department of Electrical and Computer Engineering:

It is my pleasure to write to you this letter in support for Dr. Mohit Tiwari's Tenure and Rank Advancement Promotion case. I fully champion Dr. Tiwari's promotion given his strong research record, as I substantiate below.

I am a principal research scientist at Visa Research, a research lab part of Visa Inc. focusing on systems and application security, where I also lead the systems security research group. Visa is a strong proponent and significant user of hardware-based security at all levels of its worldwide payment processing system. As payments and other currency transactions migrate from proprietary networks to the Internet and from proprietary hardware endpoints to general-purpose and embedded computing devices, cyber attackers are likely to increase their efforts to breach payment systems, to inject fraudulent transactions, and to launch denial-of-service attacks. Developing architectures, mechanisms, and techniques to secure open payment networks that power world commerce is a significant priority for Visa.

I have known Dr. Tiwari for about four years, first meeting him at a security conference and then pursuing collaboration with him on a variety of topics. At the time I was a senior researcher at Qualcomm's research lab in Silicon Valley (QRSV) and one of my lab's research areas was hardware-enhanced malware detection. Dr. Tiwari and I quickly converged on problems of joint interest, exchanging ideas and brainstorming, and later on having one of his students, Mikhail Kazdagli, visit QRSV as an intern. In 2017 I moved to Visa Research and Dr. Tiwari and I brainstormed about the novel approach of data-centric security, with both me visiting his lab at UT Austin and him visiting my lab in Palo Alto, CA. In short, I am familiar with Dr. Tiwari's work and have been interacting with him on research topics for a number of years, and thus I consider myself to be well qualified to comment on his scientific contributions.

Dr. Tiwari has published significant research results in multiple domains, from side channels, to hardware-based isolation, to secure architectures for privacy. His publications appear in top conferences such as ACM CCS, USENIX Security, MICRO, HPCA, ASPLOS, and ISCA, thus reflecting both the quality of the work and the impact of the results in the corresponding fields (security and architecture, respectively). I would like to comment on two results with which I am familiar.

The first result is in the area of oblivious RAM (ORAM), which is a concept describing algorithms and systems that protect the confidentiality of a computation and its data even when an adversary can closely observe any and all side effects. There has been tremendous effort in this space, initially to define and formalize the ORAM concept by itself, then to design algorithms and systems that implement ORAM for various types of computations. In "GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation," Dr. Tiwari and his co-authors presented a practical system that achieved a strong version of ORAM. I regard this work as a crucial contribution to the area, as the original combination of hardware and software support in the paper showed that it is possible to build efficient and secure ORAM systems. This work opened the floodgates of research into practically minded ORAM schemes, and it is likely the reason why leading technology companies (Visa Inc. included) are deploying or considering such approaches in their products and services.

The second result I would like to discuss is titled "DATS: Data Containers for Web Applications," in which Dr. Tiwari and his students introduced a new way to architect web applications that guarantees security of data while lessening the burden of application developers. In contrast to the GhostRider work, which showed that the existing theoretical idea of ORAM could be implemented efficiently, DATS is the first publication describing the fundamentally new approach of *data-centric security*. The data-centric approach holds the potential to make security more pervasive, easier to achieve for developers, and easier to verify and trust for users. DATS shows how to apply data-centric security to web applications and opens new research directions towards changing how hardware and software is designed, built, deployed, and used. Although DATS is extremely recent work and thus not fully assessed by the community, there is significant potential to this line of research and Dr. Tiwari is well positioned to lead the wave of discovery and innovation.

In comparing Dr. Tiwari's research career trajectory with those of his peers in other research-intensive universities, I see a focus in his work on tackling fundamental challenges and creating core technologies, instead of simply addressing the limitations of today's trendy technologies. Dr. Tiwari built on his early PhD work in secure hardware architectures and has since successfully established himself as a key contributor in several security domains (side channels, ORAM, intrusion detection, privacy architectures). In addition, I would like to add that I appreciate his focus on building secure systems, which are both more meaningful and more relevant to the industry, instead of limiting himself to (popular) security attacks.

I have interacted with Dr. Tiwari and his group primarily through the prism of research collaborations. Yet I have one more data point to add to this letter, related to the advising and mentoring role that Dr. Tiwari fulfills at UT Austin. As I mentioned earlier one of his students, Mikhail Kazdagli, visited my lab at Qualcomm Research. Mikhail was interested in programming language techniques for analyzing and establishing the security properties of mobile apps. At the same time, we were pursuing a new project in applying machine learning to malware detection. This project caught Mikhail's interest and, although he spent no time on the topic as an intern, he expressed interest in it once he returned to Dr. Tiwari's lab at UT Austin. Two years later I was impressed to learn, as an external member on Mikhail's PhD committee, that under Dr. Tiwari's advising, Mikhail completely switched from programming languages to machine learning for security. Such a PhD research pivot can be successful only with the help, guidance, and support of the PhD advisor and I see Mikhail's success in his PhD as a brilliant illustration of Dr. Tiwari's mentorship qualities.

Overall, I regard Dr. Tiwari as an exceptional researcher with an extensive and well-founded vision for systems and hardware security and with significant potential for future scientific advances. I understand he is also pursuing the commercialization of his research ideas and I am sure the company will be successful under his leadership. I am strongly in favor of this promotion case and I hope you will decide in his favor. If there is any additional information or insights I can provide, please do not hesitate to contact me.

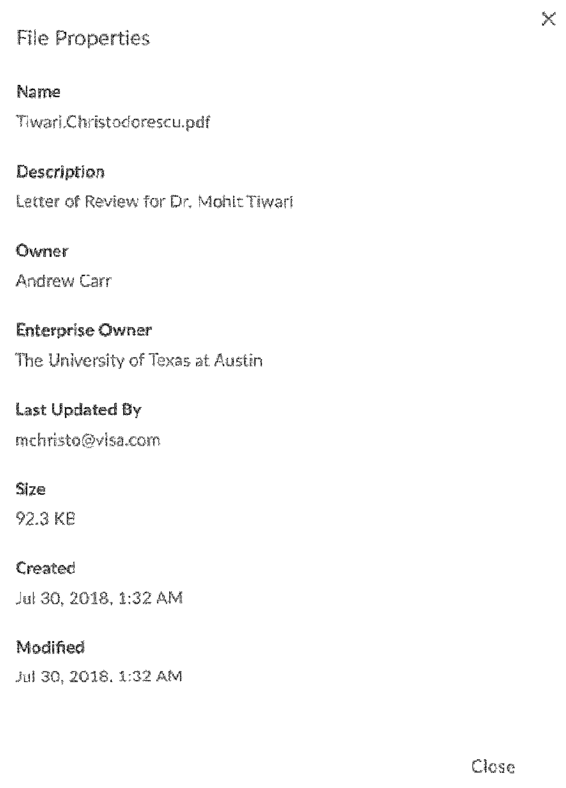
Yours sincerely,

Mihai Christodorescu

Mihai Christodorescu
Senior Director, Systems Security

Visa Research
385 Sherman Ave
Mailstop PA-1E
Palo Alto, CA 94306

mihai.christodorescu@visa.com
+1 408-239-6948
https://usa.visa.com/about-visa/visa-research/mihai-christodorescu.html



File Properties

Name
Tiwari.Christodorescu.pdf

Description
Letter of Review for Dr. Mohit Tiwari

Owner
Andrew Carr

Enterprise Owner
The University of Texas at Austin

Last Updated By
mchristo@visa.com

Size
92.3 KB

Created
Jul 30, 2018, 1:32 AM

Modified
Jul 30, 2018, 1:32 AM

Mihai Christodorescu

VISA

Principal Researcher, Security

Focus areas: Software Security, Program Analysis, and Systems Security

Research interest

I am interested in fundamental approaches to computer security and privacy problems by combining methods from multiple domains—programming languages, machine learning, behavioral modeling, and formal methods. My past and present projects have addressed Internet-scale security analysis of networks, systems, and software, and whole-system security hardening for both cloud and mobile endpoints.

Education

- 2003–2007 Ph.D. in Computer Sciences, August 2007.
  - University of Wisconsin, Madison, WI, USA.
  - Dissertation: Behavior-based Malware Detection.
  - Adviser: Prof. Somesh Jha.

- 1999–2000, 2001–2002 M.S. in Computer Sciences, Dec. 2002.
  - University of Wisconsin, Madison, WI, USA.
  - Adviser: Prof. Somesh Jha.

- 1996–1999 B.S. (High Honors) in Computer Science, May 1999.
  - University of California, Santa Barbara, CA, USA.

C

ELECTRICAL ENGINEERING AND COMPUTER SCIENCE
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Srini Devadas, Edwin S. Webster Professor of EECS 617.253.0454
32-G844, The State Center Fax 617.253.6652
Cambridge, MA 02139-4307 devadas@mit.edu

July 20, 2018

Prof. Ahmed Tewfik
Chairman
Department of Electrical and Computer Engineering
University of Texas, Austin

Dear Prof. Tewfik,

It is a pleasure to write a letter in strong support of Prof. Mohit Tiwari's promotion to Associate Professor with Tenure at the University of Texas at Austin. I am intimately familiar with his work in computer security and computer architecture.

Mohit's work first came to my attention through my reading of the Phantom publication (2013). My group had been working on a similar secure processor called Ascend concomitantly. While we had published on Ascend a bit earlier, our results were simulation based, whereas Phantom was a Field Programmable Gate Array (FPGA) implementation. The cryptographic primitive in Phantom, Path ORAM is quite a complex primitive, and it was most impressive that Mohit and collaborators were able to implement it efficiently in hardware. I should emphasize that there were excellent design choices and algorithmic changes made in Path ORAM to make it amenable to hardware implementation. The Phantom paper motivated us to develop our own FPGA implementation of Ascend and eventually a custom silicon implementation. We drew from several ideas in the Phantom paper.

In 2015, Mohit was involved in two groundbreaking papers that made oblivious computation practical. First, GhostRider is a co-designed compiler and architecture for supporting privacy preserving computation in the cloud. Its goal is memory trace obliviousness, which is provided by Phantom using a single ORAM over the entire memory space. The key observation is that it is not necessary to use ORAM; GhostRider uses program analysis to allocate data to non-oblivious, encrypted RAM when doing so does not compromise memory trace obliviousness. The use of multiple, smaller ORAM banks also significantly improves performance. The GhostRider hardware and compiler significantly outperform Phantom and Ascend, since the computations are shrunk in complexity.

The second effort was called Racoon, which uses a completely different way of achieving resistance to side channel attacks. The key insight is that all digital side channels emerge from variations in program execution and rather than balancing program execution paths to not leak information about which path was taken, Racoon executes extraneous program paths, termed decoy paths, to obfuscate program execution. Racoon's goal is to make the adversary's view through any digital side-channel appear the same as if the program were run many times with different inputs. To ensure that the system records the output of only the real path and not the decoy paths, Racoon uses a transaction-like system to update memory. Racoon is almost an order of magnitude faster than GhostRider, making it a practical way of achieving secure computation. Phantom, GhostRider and Racoon are systems that combine great ideas with great execution, and have significantly moved state of the art in oblivious computation.

As mentioned above, Phantom and Ascend use ORAMs for oblivious computation. They have high overheads that can be reduced through the compiler and program transformation techniques that Mohit developed. But what if we cannot modify the code? Mohit has looked into oblivious computation where ORAM overheads can be significantly reduced by moving some ORAM functionality into the memory system. With collaborators, he designed a secure DIMM using commodity memory and a key-equipped buffer chip. If these secure DIMMs are assumed, then new ORAM protocols can be used that reduce bandwidth, latency and energy per ORAM access. The protocols developed are non-trivial; each secure DIMM is responsible for part of the ORAM tree, and ORAM operations are performed in parallel. The main memory channel bandwidth is reduced because only a small subset of the many shuffle operations needed by conventional ORAM need to be performed. Importantly, the new protocols guarantee the same obliviousness properties as Path ORAM, while improving performance by 2X over the best available ORAM schemes.

In the field of secure architecture, in my opinion, Mohit has done the best work of anyone in his age group (or pre-tenure) over the past several years. I quite dislike work with *ad hoc* security "guarantees" that tries to sell itself through improved performance. If we have learned anything over the years it is that these *ad hoc* guarantees invariably fail the test of time. Mohit's work stands out because he builds the "right" kind of systems, where at least the specification of the systems can be proven to have strong security guarantees that are convincing to system security and cryptography researchers alike.

I therefore give Prof. Mohit Tiwari my strongest recommendation for promotion to Associate Professor with Tenure at UT Austin. Please feel free to contact me if you have any further questions.

Sincerely yours,

S. Devadas

Srini Devadas
MacVicar Faculty Fellow

Jilda Bolton

Subject: FW: Response needed by Friday 6/8: would you be able to provide a letter of reference in support of the promotion of Prof. Tiwari to associate professor by July 27?
Attachments: mohit-tiwari.pdf; Untitled attachment 00258.html

Resent-From: <tewfik@austin.utexas.edu>
From: Srini Devadas <devadas@csail.mit.edu>
Date: July 20, 2018 at 3:30:23 PM CDT
To: "Tewfik, Ahmed H" <tewfik@austin.utexas.edu>
Cc: "Erengil, Jac" <jac.erengil@utexas.edu>
Subject: Re: Response needed by Friday 6/8: would you be able to provide a letter of reference in support of the promotion of Prof. Tiwari to associate professor by July 27?

Dear Ahmed,

Please see attached letter (signed PDF).

regards

Srini

Srini Devadas

Webster Professor of Electrical Engineering and Computer Science

Massachusetts Institute of Technology

Srini Devadas is the Webster Professor of Electrical Engineering and Computer Science and has been on the MIT EECS faculty since 1988. He served as Associate Head of the Department of Electrical Engineering and Computer Science, with responsibility for Computer Science, from 2005 to 2011.

Devadas's research interests span Computer-Aided Design (CAD), computer security and computer architecture and he has received significant awards from each discipline. In 2015, he received the ACM/IEEE A. Richard Newton Technical Impact award in Electronic Design Automation. He received the IEEE Computer Society Technical Achievement Award in 2014 for inventing Physical Unclonable Functions and single-chip secure processor architectures. Devadas's work on hardware information flow tracking published in the 2004 ASPLOS received the ASPLOS Most Influential Paper Award in 2014. His papers on analytical cache modeling and the Aegis single-chip secure processor were included as influential papers in "25 Years of the International Conference on Supercomputing." In 2017 he received the IEEE W. Wallace McDowell Award for contributions to secure hardware. He is an IEEE and ACM Fellow.

Devadas has taught widely in EECS, lecturing classes in VLSI, discrete mathematics, computer architecture, algorithms and software engineering. He is a MacVicar Faculty Fellow and an Everett Moore Baker teaching award recipient, considered MIT's two highest undergraduate teaching honors.

UNIVERSITY OF CALIFORNIA, SANTA BARBARA

BC

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO

SANTA BARBARA • SANTA CRUZ

DEPARTMENT OF COMPUTER SCIENCE

SANTA BARBARA, CALIFORNIA 93106

Christopher Kruegel
Professor, Department of Computer Science
University of California, Santa Barbara
Home: `https://www.cs.ucsb.edu/~chris/`

August 20, 2018

To whom it may concern:

I am a professor in the Computer Science Department at the University of California, Santa Barbara (UCSB). I write this letter to strongly recommend the promotion of Mohit Tiwari to associate professor with tenure. Although I have never worked directly with Mohit, I have known him and his work for many years. Mohit has been a graduate student at UCSB who was working on security topics. Given that this is my area of expertise, I took a natural interest in his work and followed his progress. After his graduation, he has continued to publish at security venues, and I frequently meet him and see presentations about his work at conferences.

Mohit's research focuses on the intersection between computer architecture and systems security. That is, he is interested in solving real-world security problems that have significant impact, and he does so by considering the entire computing stack from the hardware up to the application layer. This is a rare but important viewpoint. Most security research assumes that the underlying hardware is secure and can be fully trusted. Unfortunately, as recent exploits such as Spectre and Meltdown have demonstrated, this assumption is often not true. Moreover, by looking at the hardware level, it is also possible to build into the underlying platform security mechanisms that layers above can leverage to build security primitives that are more effective and efficient.

Looking at Mohit's recent papers, I am probably most familiar with his work on malware detection. Malware analysis and detection is a topic that is near and dear to my heart, and I have published in the area for at least 15 years. Mohit focused on hardware-based malware detectors (HMDs), which are a type of behavioral malware detectors. A HMD observes program execution by looking at CPU instructions and micro-architectural traces. An alert is raised when the current trace's statistics sufficiently deviate from benign traces (unsupervised HMDs) or look similar to known malicious traces (supervised HMDs). HMDs are small, secure even from a compromised OS, and can detect attacks that leave no system call traces. They are thus a trustworthy first-level detector in a network-wide malware detection system. In his work on Sherlock, Mohit first carefully evaluated existing HMDs under a broad range of operational constraints. Moreover, he specifically looked at the robustness of existing techniques against obfuscation and malware that deliberately attempts to evade detection. Based on the observations and learnings during this evaluation, he then proposed additional, novel features that significantly improved the capabilities of HMDs.

Mohit has also done work on data containers at the (web) application level. I specifically would like to point out his DATS paper in that regard. Data containers enable users to control access to their data while untrusted applications run on it. Building usable and efficient data containers is a challenging problem. The DATS work introduced an interesting mix of hardware-capability-enhanced containers and two new primitives – modeled after the popular model-view-controller (MVC) pattern – to address these usability and performance challenges. Whenever scientists propose new programming primitives, there are always questions around feasibility and practicality. However, Mohit's evaluation, where he applies the new techniques to real-world programs such as Gitlab, convincingly addresses these concerns and shows that the approach has clear real-world potential.

Mohit is a prolific researcher with a strong publication record. He has published more than 30 papers, many in top venues. From example, he has published three papers in the top-4 security conferences (2x Usenix Security and 1x ACM CCS). Moreover, he has multiple papers in top architecture conferences (such as ASPLOS and MICRO) and a paper in a top programming languages conference (PLDI). All these venues are extremely competitive and have very low acceptance rates. In addition, what is very impressive is the broad range of Mohit's work and the fact that he can publish in a variety of venues that span different areas.

A strong confirmation of Mohit's outstanding scholarly achievements are the awards that he has received. In particular, I would like to point to the NSF CAREER award, which is given to top assistant professors who show significant promise. Moreover, he received a best paper award at ASPLOS, a best paper award at the International Conference on Parallel Architectures and Compilation Techniques (PACT), a best paper runner-up award at the International Symposium on Hardware-Oriented Security and Trust (HOST), and several IEEE Micro Top Picks of the Year. This is an impressive list of awards for a young scientist.

Mohit has a solid track record of serving on the program committees of top conferences (such as ASPLOS, ACM CSS, and the IEEE Symposium on Security & Privacy). Given that he is invited year after year to PCs, it is clear that his opinion and service is highly valued. In addition, he has been selected to serve as an Associate Editor for ACM Transactions on Architecture and Code Optimization (TACO), a top journal in the field. This is a nice recognition and testimony to his standing in the community.

Looking at his CV, I see that Mohit has won a number of research grants in the last few years, with a funding total of more than two million USD for Mohit alone. Given the tough funding environment and the difficulties of many agencies to find money, this is a great achievement. The research funding allows Mohit to support a well-sized research group, and I am happy to see that he works with a good number of PhD students. Systems security and computer architecture are areas where a significant amount of work needs to be spent building software artifacts. For this, students are a necessary and important resource. Working with seven PhD students as well as master students will allow Mohit to get the work done that he needs to turn his research vision into reality.

In summary, I think that Mohit is an outstanding scholar and a recognized leader in the group of researchers who focus on computer security and architecture. He has demonstrated his ability to perform first class research on topics that have real-world impact. Thus, I strongly recommend him for promotion to associate professor with tenure. I also have no doubt that his promotion would be fully supported by the faculty at our institution. Please let me know if you have any questions or require additional information.

Sincerely,
Christopher Kruegel

From: Christopher Kruegel <chris@cs.ucsb.edu>
Sent: Monday, August 20, 2018 5:41 AM
To: Erengil, Jac <jac.erengil@utexas.edu>
Subject: Re: Tiwari Promotion Letter

Jac,

I am sorry for the delay. Please find attached the PDF of my letter for Mohit. Please let me know if the format works or if you need anything else.

Thanks, and again, sorry for the delay.

Best regards,
Christopher

Christopher Kruegel

Professor, University of California – Santa Barbara

Bio

I am a Professor in the Computer Science Department at the University of California, Santa Barbara. My research interests are computer and communications security, with an emphasis on malware analysis and detection, web security, and security in social networks. I enjoy to build systems and to make security tools available to the public. I have published more than 100 conference and journal papers, and I am a recent recipient of the NSF CAREER Award, the MIT Technology Review TR35 Award for young innovators, an IBM Faculty Award, and several best paper awards.

Research

The main focus of my research is systems security. I seek to create solutions that solve important security issues affecting a large number of users. The goal of my work is to build security systems, deploy them in real-world environments, and perform experiments to characterize and explain their behavior. I believe that creating working systems that address real-world problems not only provides a great incentive for my research, but also allows for the necessary sanity checks of the results. As part of my research, I have contributed to systems that analyze programs to determine whether they are malicious or not (both for x86 binaries and mobile phone application). I have also worked on systems that scan the code of web applications to find vulnerabilities. Finally, I have worked on novel ways to break privacy on social networks as well as on ways to improve them such that those attacks no longer work.

UNIVERSITY OF CALIFORNIA, BERKELEY

BC

BERKELEY • DAVIS • IRVINE • LOS ANGELES • RIVERSIDE • SAN DIEGO • SAN FRANCISCO SANTA BARBARA • SANTA CRUZ

PROFESSOR JOHN KUBIATOWICZ
673 SODA HALL #1776
BERKELEY, CA 94720-1776

EMAIL: KUBITRON@CS.BERKELEY.EDU
PHONE: (510) 643-6817
CELL: (510) 872-6092

August 19th, 2018

Re: Promotion Case for Mohit Tiwari

I am pleased to write this letter in support of Mohit Tiwari's promotion case. As I detail below, I believe that Mohit has a compelling research agenda and has more than demonstrated the ability to succeed at a top-notch university such as UT Austin. In short, it is my recommendation that UT Austin should take the step of advancing Mohit to the rank of Associate Professor with Tenure.

I have known Mohit for 5 or 6 years now. I first encountered him as a post-doc at UC Berkeley, where he and I collaborated on the PHANTOM Oblivious RAM (ORAM) work. Initially, we interacted through my graduate student, Martin Maas (a co-author on that PHANTOM paper), but eventually started chatting in my office about a wide array of topics from security, to computer architecture, to software engineering. It was clear at that time that Mohit had a keen intellect and firm grasp of a variety of areas of computer science. The PHANTOM work was fascinating to me because it introduced me to a whole new class of security concerns that I had not previously considered, namely the fact that visibility of address traces could reveal significant information about the computation that was running on the local processor – even if the data was encrypted. Of course, the expense of various solutions to this problem (such as ORAM) was also quite interesting. PHANTOM was clearly the first step to a much bigger research agenda. Those discussions with Mohit were quite enjoyable, as I recall, and I could tell that he was going to make a great cross-disciplinary researcher.

Fast-forward to today, and I see that my initial impressions have been born out. Mohit has positioned himself at a difficult but extremely important interface between hardware, operating systems, algorithms, and security. His chosen focus – security of computational systems in the context of covert channels and malware breaches – might once have considered a bit "boutique" and only for the truly paranoid. However, the last few years have been truly eye-opening for many. For instance, I don't think that anyone was expecting the magnitude of the so-called Spectre/Meltdown hardware breaches, which demonstrated that many of the mechanisms that computer architects had developed to improve performance (e.g. caching and branch-prediction to name just two) were suddenly exploitable to violate the security of data within the kernel. In their 2018 Turing award lecture, Dave Patterson and John Hennesey declared that a whole new research agenda was necessary to figure out how to extract performance from hardware without risking a wide array of covert timing channels. Amidst such revelations is the fact that every day seems to bring a new data breach: Equifax, Facebook, Target, to name a few, We clearly have a crisis of cyber security.

Mohit's agenda strikes at the heart of these problems: focusing on Data Centric design, information flow control, detection or elimination of covert channels, as well as cryptographically hardened memory and computational systems. What makes these issues so hard to address is that timing channels are extremely difficult to eliminate – especially when adversaries are allowed to observe parameters such as power, address traces, or access timing. Precisely since these problems are so hard to address, only a researcher who can cross many different levels of abstraction can hope to find solutions. Looking through Mohit's recent papers, I am impressed with the *breadth* as well as *depth* of his papers: from (1) power-analysis of gate-level circuits for key exchange in lattice cryptosystem; to (2) compiler techniques for analyzing the flow of secret information; to (3) automatically executing multiple conditional paths to remove the effect of secure information on control flow, to (4) information-theoretic analysis of the capacity "contention-based" channels between co-resident virtual machines; to (5) hardware-based malware detectors; to (6) exploiting MVC ("Model/View/Control") programming models to ease the burden of programming in a data-centric environment. Mohit strikes me as a systems architect with a capital "A": cross-disciplinary, cross abstraction boundary architecture. Although working across abstraction boundaries has always been the mark of a good architect, the ability to move fluidly across boundaries is particularly important for a secure systems architect such as Mohit[1]. Further, Mohit seems to collaborate within and across institutions – a trait that I would view as extremely positive for one who wishes to tackle cross-disciplinary issues (not to mention being a great personality trait as a departmental colleague).

Mohit has a nice balance of finished and ongoing work. Just glancing at his CV, his last 5 years have been fairly productive in targeting top-tier conferences: ASPLOS (3 papers), MICRO (2 papers), HPCA (2 papers), USENIX Security (2 papers), as well as others. Mohit's paper count may be a bit lower than others in a similar position, but I'd say that it is more than sufficient, *especially since these papers are not merely least-publishable units* (LPUs). In many cases, they are full-stack implementations that implement everything from hardware to software systems, compilers, and programming environments. Such systems take time to build and each paper represents a significant amount of work. In other cases, Mohit and his students have produced focused, well-characterized experiments to study particular artifacts.

A few thoughts on Mohit's current work is as follows: First, in the category of complete system implementations, is a sequence of systems: PHANTOM, GhostRider, and Racoon. These systems share a common theme: replacing secret-data-dependent execution with static control and dataflow to remove the potential for information leakage. The result of such obfuscation is invariably expensive, but seems to get less expensive with each system that Mohit designs: although still expensive, Racoon provides significant performance improvements over the previous two systems (and state of the art). These works propose new instruction sets (implemented within the RISC-V processor environment), compilers, and programming annotations to achieve their results. I look forward to seeing how this work evolves – especially since I've just embarked on a data-centric research agenda myself. As a side note, I thought that his paper on moving the ORAM primitives closer to memory ("Secure DIMM: Moving ORAM Primitives Closer to Memory") was an interesting proposal to supplement the rest of this work.

Second, Mohit has been studying a number of different covert channels, including "contention-based" channels between different processes (or containers) on the same machine. These channels exploit contention for some resource such as the cache. I thought that the paper characterizing these channels ("Understanding Contention-Based Channels and Using Them for Defense") was novel and interesting. Studying such channels and their information-theoretic capacity, followed by investigating ways in which these channels could be made robust to interference from other processes was an interesting angle. In the same vein, Mohit has been studying information leakage in "Post-Quantum Key Exchange" algorithms (i.e. for lattice cryptosystems). This research involves building circuits to perform the key exchange, and performing differential power analysis (DPA) to demonstrate the significant vulnerability of such circuits to power analysis. Given the

[1] Mohit works at many levels, so that simply calling him a "security researcher" or "computer architect" or "language designer" would probably not do him justice. I settled on "secure systems architect."

current industrial push in Quantum computing, I thought that studying such channels was timely and quite interesting.

Third, Mohit's work on DATS (a programming framework for web applications that respects data access control) seems like a very interesting future direction to help prevent data breaches. One of the difficulties of many data-centric programming frameworks is that they can become very difficult for application writers to balance the granularity of access control with programmability. I can see how this framework might provide a happy medium for web-based applications. According to Mohit's research statement, this work is already being adopted in industry – a clear sign that it addresses an industry-visible need.

Finally, the anomaly detection work (as represented, for instance, by his study of hardware-based malware detectors) seems like a potentially impactful research direction, one that will be interesting to follow as it develops.

In summary, I think that UT Austin should promote Mohit Tiwari to the rank of Associate Professor with Tenure. He has chosen a challenging but important area in which to focus his research: secure systems design in the face of covert channels and malicious observers. He seems to have the skills that he needs to succeed at building systems across many levels of abstraction: from hardware (digital circuits and computer architecture), to operating systems, to compilers, to application frameworks. He seems comfortable with tools of the trade such as cryptography, information theory, and differential power analysis to name a few. I would say that he is a well-rounded researcher and would make a good long-term colleague for the Department of Electrical and Computer Engineering at UT Austin.

Please feel free to contact me with any additional questions. My contact information is in the header of the first page of this letter.

Sincerely,

Prof John Kubiatowicz
EECS, UC at Berkeley

From: John Kubiatowicz <kubitron@cs.berkeley.edu>
Sent: Monday, August 20, 2018 12:03 AM
To: Tewfik, Ahmed H <tewfik@austin.utexas.edu>
Cc: kubitron@cs.berkeley.edu; Erengil, Jac <jac.erengil@utexas.edu>
Subject: Re: Faculty Promotion Letter Due, UT-Austin

Ok, please see attached letter.

Sorry again for the delay. I apologize if it is a bit too short or not what you need.
--KUBI--

On 8/16/2018 8:43 AM, Tewfik, Ahmed H wrote:
That would be fine Kubi. Thank you!

regards
Ahmed

Professor John Kubiatowicz Biography
University of California, Berkeley

John Kubiatowicz received a double B.S. in Electrical Engineering and Physics, 1987, M.S. in Electrical Engineering and Computer Science, 1993, and a PhD in Electrical Engineering and Computer Science. Minor in Physics, 1998, all from M.I.T.

He joined the faculty of EECS at UC Berkeley in 1998. Current research includes exploring the design of extremely-wide area storage utilities and developing secure protocols and routing infrastructures that provide privacy, security, and resistance to denial of service, while still allowing the caching of data anywhere, anytime. Also, exploring the space of Introspective Computing, namely systems which perform continuous, on-line adaptation. Applications include on-chip tolerance of flaky components and continuous optimization to adapt to server failures and denial of service attacks.

Honors and awards include the Diane S. McEntyre Award for Excellence in Teaching, 2003, Scientific American 50, 2002, Mounds View High School Distinguished Alumni Award, 2001, Berkeley IT Award for Excellence in Undergraduate CS Teaching, 2000, Presidential Early Career Award for Scientists and Engineers (PECASE), 2000, George M. Sprowls Award for best PhD thesis in EECS at MIT, 1998, IBM Graduate Fellowship, 1992 -1994, and Best Paper, International Conference on Supercomputing, 1993.

Research Areas

Computer architecture
Quantum computer design
Internet-scale storage systems
Peer-to-peer networking

BC

COLLEGE OF ENGINEERING
COMPUTER SCIENCE & ENGINEERING
UNIVERSITY OF MICHIGAN

August 1, 2018

Ahmed Tewfik
Cockrell Family Regents Chair in Engineering
Chairman, Department of Electrical and Computer Engineering
The University of Texas at Austin
2501 Speedway Ave.
EER 2.876
Austin, TX 78712

Dear Prof. Tewfik,

It gives me pleasure to write this letter of assessment for the appointment of Prof. Mohit Tiwari to the position of Associate Professor with Tenure in the Department of Electrical and Computer Engineering at The University of Texas at Austin. I am an avid follower of Prof. Tiwari's research, but have not collaborated with him. We both work in the area of computer architecture and attend many of the same conferences. This is how I got to know his work and have followed it over the years. We were also both part of the DARPA sponsored Center for Future Architectures (CFAR) from 2015-2017, thus I got to see him on a regular basis at our quarterly reviews.

Before proceeding further, let me summarize my background and qualifications. I am a Professor in the EECS Department at the University of Michigan. I joined Michigan in 2001 after spending 6 years at Hewlett Packard Laboratories as a Research Scientist. I got my Ph.D. in Electrical Engineering from the University of Illinois at Urbana-Champaign in 1997. My area of research is computer architecture and compilers, with specialization in low power computing, application-specific processors, and reliability where I have published more than 200 conference and journal papers. I lead the Compilers Creating Custom Processors research group at Michigan with funding from ARM, Samsung, Intel, Huawei, DoE, DARPA, and the National Science Foundation. To date, 27 Ph.D. students have graduate from my group and are employed at Intel, AMD, Google, Facebook, Apple, ARM, Synopsys, Indiana University, and Hanyang University.

Overall Assessment: Prof. Tiwari is an excellent researcher in the areas of computer architecture and software systems. He is best known for his work in integrated hardware/software security solutions with particular emphasis on side channel attacks where he has become one of the most respected and a true leader in the area. His research record is impressive with a long list of top-tier conference publications in the area of computer architecture and security. This includes Best Paper Awards at ASPLOS and PACT and two IEEE MICRO Top Picks selections. Tiwari has a deep technical knowledge in the fields of hardware and software security, combined with a creative mind that allows him to develop innovative solutions to challenging research problems. He is self-motivated and takes a strong initiative to his research, teaching, and service. I am impressed by his abilities to innovate across the traditional hardware/software boundaries as well as develop industry-relevant solutions that can have a real impact on tomorrow's products. He is a dedicated scholar who is happy to talk technical with almost anyone from senior faculty to new graduate student. I firmly believe that Tiwari will be a strong asset to the ECE Department at UT Austin for many years to come.

Research Contributions and Impact: Prof. Tiwari's research focuses on building secure computer systems, specifically hardware/software security solutions. Security of personal data is a critical problem that the computer industry and government agencies are heavily investing in, thus for a faculty member, it is a great space to work. Interestingly though, relatively few faculty in the computer architecture area actually work on security, which makes Prof. Tiwari a valuable and highly sought after individual for his unique expertise.

Tiwari is best known for his work on side-channel attacks, wherein digital information is unknowingly leaked through the hardware or operating system. One of his important insights is that the leaks arise when program execution varies based on the content of the secret information. If the program execution differences could be masked, then these leaks would disappear. His work on decoy execution accomplishes exactly this goal by creating "decoy" executions to hide the secret-dependent program execution. On the surface, this solution makes intuitive sense, but it is actually very challenging to create decoys that do not cause program crashes as the program was designed to have specific data-dependent behavior. Tiwari and his collaborators developed an automatic methodology to systematically create decoy paths that are guaranteed to run without crash and properly obfuscate the secret-dependent behavior. This work was published at the 2015 and 2016 USENIX Security Symposia, the top conference in security. I am impressed by this work because of both the difficulty of the problem solved as well as the rigor and completeness of the solution. Further, the solution is a software solution, but requires strong knowledge of the hardware to understand how the information leaks, thus it truly showcases Tiwari's strengths in both software and hardware.

More recently, Tiwari began a thread of research that focuses on a more data-centric approach to security for web-applications. Rather than protecting data by ensuring applications use the data more properly, his approach is to protect the data explicitly, regardless of the usage, by using strict access control rules for the data. His approach, called DATS and published at the ASPLOS 2018 conference, takes a user's access control policies and translates them to information flow control on arbitrary web applications. Thus, even if these applications are untrusted or have been compromised, they cannot leak data to an unauthorized user or unknown server. The approach is elegant, timely, highly practical, and seems destined to be adopted by the industry as it just makes too much sense. This work showcases Tiwari's inherent ability to identify and solve some of the most critical research problems. It also demonstrates that he is a true innovator who can think outside the traditional box to solve some of the most critical security problems that we face.

Teaching Contributions: While I have never seen Prof. Tiwari teach in person, his record at UT Austin is strong. Of particular note is his undergraduate embedded systems class. This is a lab-focused class with more than 300 students in it, which is amazingly large. His ability to manage this many projects and keep the class accessible and engaging to such a wide range of students is truly impressive. It is evident that he cares deeply about the students and this comes across in his lectures and one-on-one interactions. He is also an excellent presenter who does a great job of combining principle with practice so that the students understand why they are learning something and where it is used in the real world. It is clear to me that Tiwari is a strong asset to the department in teaching now and into the future.

Service to the Broader Community: Prof. Tiwari also has an excellent service record. He regularly serves on technical program committees for the top conferences in the computer architecture area including ASPLOS, HPCA, ISCA, and MICRO. I had the pleasure of serving on the ASPLOS 2018 program committee. I was struck by the strength of his reviews, each reflecting significant effort and careful thought. His comments during the PC meeting were well articulated, right on target, and substantiated by his strong knowledge of the broader research space. I also appreciated that while he had his own opinions on papers, he demonstrated respect of other opinions even if he did not agree and engaged in thoughtful discussions of controversial papers. I would not hesitate to invite him to any a future program committee that I chair as hard working, diligent, and well-reasoned committee members are invaluable and often hard to find. Overall, Prof. Tiwari's service roles provide excellent visibility for his research program, and he is on the right trajectory for his future career.

Final Recommendation: After careful evaluation of Prof. Tiwari's contributions to research, teaching, and service, I conclude that Prof. Mohit Tiwari is more than qualified to be promoted to the rank of Associate Professor with tenure. His research success is evidenced by a large set of publications in the most respected conferences in computer architecture and security. He has an impressive funding record with a range of grants from NSF, DARPA, and a long list of companies (Qualcomm, Samsung, General Dynamics, Google, Huawei, Samsung, and Lockheed Martin). His early track record in both teaching and external service demonstrates a strong commitment to UT students and the broader community. At my institution (Michigan CSE), I believe that he is above the bar for tenure and we would be happy to hire him. If there is any additional information that I can provide on this case, please do not hesitate to contact me.

Sincerely,

Scott Mahlke
Professor
Electrical Engineering and Computer Science Department
University of Michigan
Email: mahlke@umich.edu
Tel: (734) 936-1602

Resent-From: <tewfik@austin.utexas.edu>
From: Scott Mahlke <mahlke@umich.edu>
Date: August 2, 2018 at 4:46:09 AM GMT+2
To: "Tewfik, Ahmed H" <tewfik@austin.utexas.edu>
Cc: "Erengil, Jac" <jac.erengil@utexas.edu>
Subject: Re: Response needed by Friday 6/8: would you be able to provide a letter of reference in support of the promotion of Prof. Tiwari to associate professor by July 27?

Ahmed, Jac,

Please find attached my Prof. Tiwari. Sorry that it is a few days late, hopefully not too late.

Regards,
Scott

Scott Mahlke
Professor & Associate Chair
Electrical Engineering and Computer Science Department
University of Michigan

INTRODUCTION

Scott Mahlke is a Professor in the Electrical Engineering and Computer Science Department at the University of Michigan. He is affiliated with the Advanced Computer and works in the areas of Compilers and Computer Architecture. He joined Michigan in 2001 after receiving his Ph.D. from the University of Illinois and working at HP Laboratories.

RESEARCH INTERESTS

My research interests lie in the areas of: compilers, computer architecture, and high-level synthesis. Specifically, my students and I focus on designing the next generation computer systems that overcome challenges in performance, power consumption, and reliability.

HONORS & AWARDS

- Received a National Science Foundation CAREER Award for his proposal entitled "Compiler-Directed Synthesis of Application Specific Processors" in 2003. NSF CAREER awards recognize and support the early career-development activities of "those teacher-scholars who are most likely to become the academic leaders of the 21st century."
- Appointed Morris Wellman Faculty Development Assistant Professor in 2004. The professorship is to be awarded to a junior faculty member to recognize outstanding contributions to teaching and research.
- 2006 ISCA Most Influential Paper Award was awarded for the 1991 ISCA paper entitled, "IMPACT: An Architectural Framework for Multiple Instruction Issue Processors." This award recognizes the paper from the ISCA Proceedings 15 years earlier that has had the most impact on computer architecture.
- Received 2007 Young Alumni Award from the ECE Department at the University of Illinois at Urbana-Champaign.

C

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Professor Onur Mutlu
Department of Computer Science
ETH Zürich
CAB F 74.2
Universitätstrasse 6
8092 Zürich
Switzerland

Phone +41 44 632 88 53
Fax +41 44 632 10 59
onur.mutlu@inf.ethz.ch
https://users.ece.cmu.edu/~omutlu/

August 18, 2018

Dr. Ahmed Tewfik
Cockrell Family Regents Chair in Engineering
Chairman, Department of Electrical and Computer Engineering

Dear Professor Tewfik:

I am writing this letter in response to your request for my assessment of Dr. Mohit Tiwari's scholarly contributions with respect to his tenure and advancement to the rank of Associate Professor at the University of Texas at Austin.

I have known Dr. Tiwari (Mohit) for almost eight years, since when he was a postdoctoral researcher at UC Berkeley and followed his research on and off since when he was a PhD student before. Although I never worked with him directly on research, I interacted with on several occasions in person at conferences and various professional meetings. I have also collaborated briefly with Mohit to present in a Special Session of the Design Automation Conference in 2016, entitled "Who Is the Major Threat to Tomorrow's Security? You, the Hardware Designer". We presented on different topics (myself on RowHammer, Mohit on the side-channel vulnerabilities and solutions; and Wayne Burleson from AMD on hardware trojans) and co-wrote an invited paper for the session (https://people.inf.ethz.ch/omutlu/pub/hardware-security-threats-invited-paper_dac16.pdf). I am also familiar with some of his works through this brief collaboration and various presentations of his that I listened to.

Overall, Mohit has become an established researcher in the critical area of hardware security. His works are novel, well done, cover a wide range of important topics in information security in hardware systems, and explore both new problems and new solutions. He has distinguished himself as one of the leading young researchers in hardware security, especially in the area of side channel vulnerabilities and protection. He has made strong scholarly contributions and he is poised to do even more. I, therefore, support his tenure and promotion to Associate Professor.

I will elaborate briefly in the rest of this letter on Mohit's contributions and qualifications. Due to extensive time constraints, I will have to keep the details short and hit only the most important bits, but I am happy to talk on the phone, as needed.

Mohit has made significant contributions to the discovery of and protection against *information leakage* issues in hardware (I will broadly call them as hardware side-channel vulnerabilities). Hardware side channels are particularly important vulnerabilities that are fundamental to the design of computing systems as shared resources. These vulnerabilities are likely to become more important going into the future as the frontier of hard-to-prevent security attacks is pushed increasingly inside the hardware (both processors and memory, but also other hardware components of a computing system). Mohit examined a wide variety of side channels in hardware and a variety of low-overhead solutions to them. The channels he has investigated include those in the memory controller (e.g., his CCS 2013 and MICRO 2015 works), in floating point computation units (e.g., his USENIX Security 2016 paper), in the very low-level hardware gates (e.g., his MICRO 2009, ASPLOS 2009 and ISCA 2011 works, which are part of his PhD thesis), in generalized shared resources (e.g., his HPCA 2015 work on contention-based side channels and their general treatment; his USENIX Security 2015 work on Raccoon; his ASPLOS 2015 work on GhostRider), in power consumption signals (e.g., his DATE 2018 work), and in post-quantum key exchange protocols (e.g., his HOST 2018 work). This is an extensive amount of high-quality coverage in side channel vulnerabilities and solutions, and I believe such high-quality coverage is Mohit's hallmark and major contribution to the field.

I will briefly mention Mohit's contributions in memory controllers and general shared resources as side-channels. As far as I know, Mohit is one of the first researchers who has examined *high-performance design of memory controllers* to mitigate the side-channel security vulnerabilities on the memory bus. His CCS 2013 work (PHANTOM) proposes a high-performance memory controller design that enables obliviousness in memory access traces of applications. It co-designs the Oblivious RAM (ORAM) algorithm together with the memory controller hardware, to achieve and exploit high levels of bank parallelism in main memory, which enables a much faster implementation of oblivious memory access traces. The mindset of this work is perhaps even more important than its specific new contribution: the security algorithm (i.e., the ORAM technique use to prevent side-channels by providing memory access trace obliviousness) and the hardware (i.e., the microarchitecture of the memory controller) should be co-designed to provide both high security and high performance. As such, I view this work as an important contribution in hardware security that has influenced future works. The work's impact is also clear on its own, given that it has received a healthy number of citations (> 100) from highly-visible papers that built on it, over the course of only five years. This work is also distinctive since it is likely the first practical demonstration of an oblivious processor implemented on an FPGA.

Mohit further improved upon this work with a higher performance memory controller design that provides fixed service to different threads that are sharing it and that provides partitioning of banks/ranks across threads. His MICRO 2015 work shows that a combination of carefully-designed memory access shaping, scheduling, and partitioning mechanisms employed in the memory controller can avoid information leakage from the access patterns in a shared memory controller while providing higher performance than prior secure memory controller solution that employs temporal partitioning. I believe this work is important as it pushes the state-of-the-art in side-channel-free memory controller design and closes the gap a bit more between a secure memory controller design and a high-performance one.

I also quite enjoyed and learned from Mohit's HPCA 2015 paper, which provides an information-theoretic treatment of generalized microarchitectural side channels, the first such treatment that I know of. This work shows that it is possible to achieve high amounts of information leakage through microarchitectural side channels, more so than thought was possible before. Based on a rigorous analysis of contention and its observability by an attacker, Mohit's work shows that contention-based side channel attacks can be detected and prevented using introspection mechanisms in hardware that are designed to detect anomalous contention. This is a relatively general-purpose mechanism that is promising to prevent a variety of side channel attacks that occur due to contention in various resources.

Apart from his leading status as a researcher in side-channel vulnerabilities and solutions, Mohit has several significant contributions to the area of hardware security. I am less familiar with these contributions, but based on my quick reading, they are in important areas and high-quality works. These attest to Mohit's breadth as a leading researcher in hardware security.

As a result of his high-quality technical contributions and the wide variety of coverage he has in hardware security, Mohit is regarded as a leading hardware security researcher in both the computer architecture and hardware security communities. He gets invited to program committees, speaking engagements and consulting activities in cutting-edge venues and issues. I have interacted with him in numerous occasions in such invited arrangements. All my interactions have been very positive – Mohit has excellent technical rigor and the ability to clearly and concisely communicate ideas of his own and others.

I must also mention that Mohit is quite collaborative. He has formed continuing collaborations with complementary researchers from a variety of institutions. For example, Mohit has collaborated with researchers in compilers, information theory, computer architecture, and other areas of security. I see this as a big positive especially because I strongly believe that fundamental solutions to difficult security problems require collaboration across domains in computing. I also think this is how strong research can be done in an era of increasingly difficult problems to solve in computing systems that require thinking across the layers.

In summary, I think highly of Dr. Mohit Tiwari's research and credentials as a junior professor. He is a leading junior researcher in hardware security, with a wide variety of high-quality and innovative works especially in hardware side-channel vulnerabilities and their solutions. His work has already had impact, which I believe will only continue to grow due to the importance and relevance (and the immediate criticality) of hardware security. I believe Dr. Mohit Tiwari is well qualified for promotion to Associate Professor at the University of Texas at Austin and therefore support his tenure and promotion to Associate Professor without any reservation.

Sincerely,

Onur Mutlu
Full Professor, ETH Zürich
Adjunct Professor, Carnegie Mellon University
onur.mutlu@inf.ethz.ch
https://people.inf.ethz.ch/omutlu/

From: Onur Mutlu <omutlu@gmail.com>
Sent: Saturday, August 18, 2018 6:18 AM
To: Erengil, Jac <jac.erengil@utexas.edu>
Cc: Tewfik, Ahmed H <tewfik@austin.utexas.edu>
Subject: Re: UT Faculty Promotion Letter Overdue

Dear Ahmed and Jac,

I attached my letter for Mohit Tiwari.

Thanks,
Onur

Onur Mutlu
http://people.inf.ethz.ch/omutlu/

Onur Mutlu

Adjunct Professor, Electrical and Computer Engineering
Swiss Federal Institute of Technology Zurich

Onur Mutlu is a Professor of Computer Science at ETH Zurich. He is also a faculty member at Carnegie Mellon University, where he previously held the William D. and Nancy W. Strecker Early Career Professorship. His current broader research interests are in computer architecture, systems, and bioinformatics. He is especially interested in interactions across domains and between applications, system software, compilers, and microarchitecture, with a major current focus on memory and storage systems. A variety of techniques he, along with his group and collaborators, has invented over the years have influenced industry and have been employed in commercial microprocessors and memory/storage systems. He obtained his PhD and MS in ECE from the University of Texas at Austin and BS degrees in Computer Engineering and Psychology from the University of Michigan, Ann Arbor. His industrial experience spans starting the Computer Architecture Group at Microsoft Research (2006-2009), and various product and research positions at Intel Corporation, Advanced Micro Devices, VMware, and Google. He received the inaugural IEEE Computer Society Young Computer Architect Award, the inaugural Intel Early Career Faculty Award, faculty partnership awards from various companies, a healthy number of best paper or "Top Pick" paper recognitions at various computer systems and architecture venues, and the ACM Fellow recognition "for contributions to computer architecture research, especially in memory systems." His computer architecture course lectures and materials are freely available on YouTube, and his research group makes software artifacts freely available online.

C

Cornell CIS
COMPUTING AND INFORMATION SCIENCE

Andrew Myers
Professor

428 Gates Hall
Ithaca, NY 14853-7501
t: +1 (607) 255-8597
f: +1 (607) 255-4428

August 3, 2018

Dr. Ahmed Tewfik
Cockrell Family Regents Chair in Engineering
Chairman, Department of Electrical and Computer Engineering
University of Texas at Austin

Dear Prof. Tewfik,

I am writing to evaluate Dr. Mohit Tiwari for promotion and tenure.

I have do not particularly know Dr. Tiwari personally but I have met him a couple of times in professional settings in the past couple of years. I am, however, quite familiar with several of his papers because much of my own work has been concerned with computer security, and in the past few years, I've been working on topics that overlap with his interests and past work. In particular, I've been working on timing channels and secure hardware, two topics where Dr. Tiwari has made significant contributions. You will find links to these and other papers on my personal website, http://www.cs.cornell.edu/andru.

Dr. Tiwari has made important contributions on multiple topics, but especially centered on controlling various side channels within hardware. As the recent prominent Spectre/Meltdown attacks have made exceedingly clear, modern hardware is full of side channels that can be exploited by adversaries to break the security of computing systems. These side channels include not only timing channels such as those exploited by Spectre, but also side channels that arise from the ordering of accesses to memory. Side channels based on physical effects such as power consumption, electromagnetic radiation, and acoustic vibrations are also a concern in more specialized settings where the adversary has physical access, but channels observable from software alone are more important, and these are what he's worked on.

In the last few years, Dr. Tiwari and his colleagues have been exploring methods for building hardware that does not have timing channel vulnerabilities. In the past few years there has been an exciting line of research that at the hardware level applies ideas about secure information flow that are borrowed from the software security world. The key insight is that while timing channels cannot be controlled adequately at the software level, timing channels manifest at the hardware level as explicit information flows that can be controlled either at run time or design time. Dr. Tiwari has been at the center of this work, which started with the initial work on gate-level information flow tracking and has continued with his more recent work on Caisson (PLDI 2011) and Sapper (ASPLOS 2013). I've been working on secure information flow at the language level for some time, but more recently my own research group, in collaboration with that of Ed Suh, has been doing work on statically controlling timing channels via hardware-level information flow. This effort has given me a fresh appreciation for the creativity and vision of Dr. Tiwari's work. With the growing recognition of the danger and importance of timing channels, we can expect his work to have a lasting and recognized impact on computer security.

Dr. Tiwari has also been doing important work on controlling side channels that arise from the sequence of memory accesses performed by processors, independent of the time at which those accesses occur. In many reasonable threat models, adversaries can learn which memory accesses are being performed (e.g., by creating contention for memory units). Oblivious RAM is a long-standing general solution, but for many years it came with horrendous performance overheads. Remarkably, with their award-winning papers on PHANTOM and Ghostrider, he and his colleagues have designed hardware-level ORAM implementations that hugely lower the overheads of ORAM, to the point where it becomes a practical technique. This work strikes me as another home run for Dr. Tiwari.

Beyond the truly outstanding results just described, Dr. Tiwari has been quite productive over the past few years, publishing multiple interesting and worthy papers per year in top venues across the research areas of both computer security and architecture. As you will be aware, the most prestigious publication venues in these research areas are conferences, Dr. Tiwari has been steadily publishing in top-tier conferences such as CCS, USENIX Security, MICRO, HPCA, and ASPLOS.

It is obvious from Dr. Tiwari's extensive participation on program committees for top conferences in both architecture and security that he's highly respected across multiple research communities. He has been a program committee member for multiple top conferences per year, year after year. I respect the admirable amount of service that he has done for the community — and given the high workload that these conferences generate for program committee members, I'm amazed that he has had time to do all the strong work that he has!

Clearly, Dr. Tiwari has built up a strong portfolio of original and significant research, and I see no sign that he is slowing down. His work is consistently creative, and he is connecting the security and hardware communities in ways that are important for the intellectual health of these communities and that show he is a master of both domains.

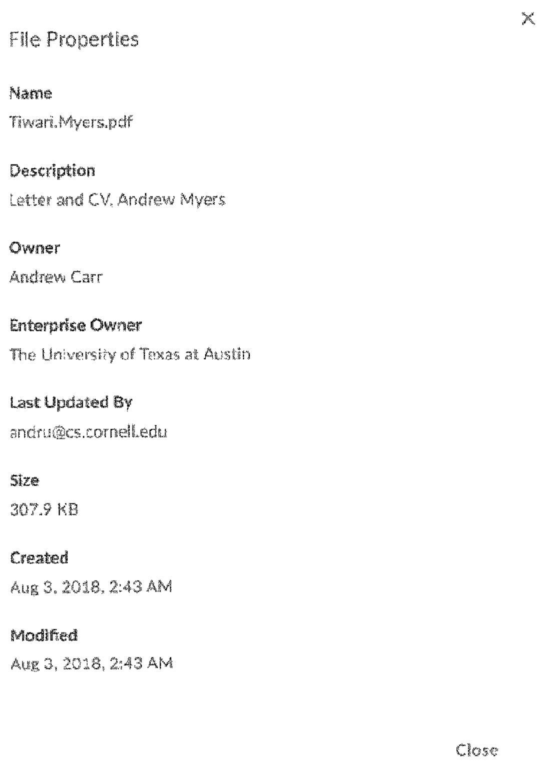
I would say that Dr. Tiwari is probably the top faculty member of his approximate academic age at the increasingly important hardware/security boundary. I don't know the architecture community as well as the security community, and evaluating him purely as a security researcher is a little unfair, but I would say he's in the same equivalence class as or a little ahead of Deian Stefan (UCSD), who also does information flow security work but at the OS and language level. He's not as productive as (his sometime co-author) Elaine Shi and Tom Ristenpart (Cornell), but then few are. I think his work is more interesting and of more lasting value than that of Alex Halderman (Michigan).

In short, I think this should be a clear case for promotion. Dr. Tiwari is doing creative, important, solid work, with at least a couple of highly important results already under his belt. He has my strong and enthusiastic support for promotion and tenure.

Sincerely,

Andrew Myers

Andrew Myers
Professor
Department of Computer Science
Cornell University



File Properties

Name
Tiwari.Myers.pdf

Description
Letter and CV, Andrew Myers

Owner
Andrew Carr

Enterprise Owner
The University of Texas at Austin

Last Updated By
andru@cs.cornell.edu

Size
307.9 KB

Created
Aug 3, 2018, 2:43 AM

Modified
Aug 3, 2018, 2:43 AM

Andrew Myers

Professor, Department of Computer Science, Cornell University

Research interests

It is too hard to build trustworthy software systems. I aim for simple, high-level abstractions that offer programmers strong guarantees about cross-cutting concerns: security, distribution, extensibility, persistence.

Current Projects

- Familia and Genus: OO languages that improve generic programming and exception handling.
- Fabric: A language and system for secure, distributed computation, sharing, and storage.
- SHErrLoc: The Static Holistic Error Locator identifies the most likely locations of program errors by analyzing the entire program constraint graph.
- SecVerilog: a hardware description language for controlling timing channels.
- Jif: an extended version of Java that enforces security and privacy by controlling information flow.
- Civitas: A practical, secure, remote voting system.
- Polyglot: a widely used, extensible Java compiler front end framework for rapid experimentation with new language extensions.
- Editor in Chief, ACM Transactions on Programming Languages and Systems (TOPLAS)

Selected recent publications

- MixT: a language for mixing consistency in geodistributed transactions (PLDI'18)

  Using information flow to enforce the consistency of atomic, mixed-consistency transactions

- Familia: unifying interfaces, type classes, and family polymorphism (OOPSLA'17)

  A lot of polymorphism and extensibility in a lightweight package

- Nonmalleable information flow control (CCS'17)

  A type system enforcing a dual hyperproperty that constrains the use of endorsement

- SHErrLoc: A static holistic error locator (TOPLAS, 2017)

  Using Bayesian principles to accurately localize errors reported by type systems and program analyses

Georgia Tech College of Engineering
School of Electrical and Computer Engineering

BC

Date: 15st August 2018

Dear Prof. Tewfik,

It is my pleasure to provide an appraisal of the qualifications of Professor Mohit Tiwari for promotion to the rank of Tenured Associate Professor. While we have not had an opportunity to collaborate, our paths have crossed may times in Program Committee meetings, conferences, and recently at the ACACES summer school in Italy last year where we were both co-instructors teaching our respective courses. Furthermore, Mohit and I were both part of the C-FAR (Center for Future Architecture Research) center at the University of Michigan. Although we were in different teams at C-FAR and our projects did not overlap, I got a chance to see Mohit and his students present their ongoing research at the center meetings. Thus, I am quite familiar with Mohit's research and can provide an objective assessment. Mohit has driven and published seminal work in secure systems. He has not only developed a top-notch research program that consistently publishes at flagship venues but also taken some of the work towards commercialization. My specific comments in this letter will describe his research contributions and offer opinions on other aspects as requested.

Research Quality: Mohit joined UT after doing highly impactful work during his graduate studies, as noted by the doctoral dissertation award and an impressive publication record at graduation. During his time as a tenure track professor, Mohit has established his own identity (distinct from his graduate advisor) and continued to have an even more impressive research record. After joining UT, he has published a dozen conference papers and that too at top venues in architecture (HPCA, ASPLOS, MICRO) and security (CCS and USENIX). His work is considered tour-de-force in building systems that are resilient to digital side channels. He has also made important contributions in the area of secure memory systems (Mohit has made are important research contributions in other areas such as Hardware-Based Malware Detectors and Data-Containers for Web Applications as well, however, I will limit my detailed comments to only two areas).

Digital Side Channels: The threat of side channels is a big concern in current computing systems, where both trust-worthy and untrusted computations can run concurrently. Digital side channels can allow the untrusted applications to infer the secret information of a co-running application by measuring information such as execution time or time to access a particular memory location. The recent side-channel attacks (Spectre and Meltdown) that affected millions of systems shows that the threat of side-channels is real and such attacks are only going to become more widespread in the future. Mohit's work on GhostRider (ASPLOS 2015) and Racoon (USENIX 2015) shows how to make secure computation resilient to side channel leaks by ensuring that the execution time of a program remains unaffected by the secret inputs to the program, thus eliminating the timing side channel leaks. Both of these contributions are very creative and original in nature, as reflected by the best paper award at ASPLOS 2015. The USENIX 2016 paper by Mohit's group shows how to make Floating Point (FP) operations consume a constant amount of time regardless of the inputs (thereby making such operations secure against timing leaks) while limiting the performance impact of the solutions by using clever approach of using empty SIMD slots. To his credit, Mohit made these key research contributions a few years ahead of time, and the architecture community is giving a serious look to these security problems only now in 2018, in response to the Spectre/Meltdown attacks.

Secure Memory System: Even if the computation incurs similar number of operations on different execution paths, the memory addresses used by a secure program can still leak information. Furthermore, the memory controller policies can allow a malicious application to infer the behavior of a victim application by doing timing-based attacks at the memory system. Mohit (in collaboration with Rajeev Balasubramonian) has tackled both of these problems with solutions that appeared at top architecture venues. To avoid information leaks at the memory controller, their MICRO 2015 paper proposes highly effective policies that rely on spatial partitioning and avoids the significant performance overheads of temporal partitioning. This research contribution is very creative in that it exploits deep insights on organization and operation of memory system. To avoid information leak on memory bus, Mohit's solutions had relied on Obfuscated RAM (ORAM). However, ORAM incurs significant performance overheads. To reduce these overheads, their recent HPCA 2018 paper looks at implementing ORAM primitives within a "Secure DIMM". These papers show that Mohit has the ability to do creative and impactful work not only on secure computation but also make solid contributions to secure memory systems. And, also that he has the ability to collaborate with outside research groups to develop effective solutions.

Impact of Research on Industry and Academia: Mohit's research contributions have had a significant impact on both industry and academia. His work on securing computation against digital side-channels and secure memory system are important contributions that are likely to receive a lot of citations and follow on research. In fact, in my own research group, my students (who are working on secure memory) have read Mohit's MICRO 2015 and HPCA 2018 papers and regard them as the state-of-the-art for their own research studies. Mohit deserves credit for leadership in this area and making research contributions well before the surge of interest that we see in secure systems due to the Spectre/Meltdown scare. What I find impressive about Mohit is that he takes the extra effort to make industrial impact based on his research work. For example, commercializing his graduate research (Tortuga Logic), or technology transfer of his Hardware-Based Malware Detector work (from UT to Qualcomm team), or doing an NSF I-Corps with his recent work on "*Data Containers for Web Applications*". Thus, Mohit's work is not only having a significant impact on the research work of other academics but it is also having an influence on the solutions being used by industry.

Quality of Funding: Mohit has been exceptional at getting funding for his research from highly respected and competitive venues. He won the NSF CAREER award, the Google Faculty award, and the Qualcomm award, all of which are highly competitive in nature. Furthermore, he was invited to the C-FAR center midway during the center primarily because of his impressive research record (C-FAR had about 20 faculty members who are considered leaders in the field, so getting invited to this group of researchers shows the respect for Mohit's research in the wider architecture community). Mohit has also received funding from the DARPA SSITH program, indicating the relevance of Mohit's research to defense programs. Overall, Mohit has a great balance of funding from federal contracts and industry, amassing an impressive 5 million dollars (with 3.6 million dollars for his part) within the short period as an assistant professor. This amount of funds from highly respected and competitive funding sources is again a testament to high quality and impact of Mohit's research work.

Service and Visibility: When I was forming my program committee for the MICRO 2015, I made it a point to invite Mohit on the committee for his expertise. It is clear from his service record that the broader research community highly values Mohit's abilities and opinion – simply note his membership on the top tier conferences in the computer architecture: ISCA (2 times), MICRO (2 times), ASPLOS (3 times), HPCA (2 times) and security: CCS (4 times), Oakland (2 times), and HOST (3 times). Mohit has served on the program committees 2-4 times for each of these top-tier conferences, which is truly impressive especially given that he is only an assistant professor. I do not know of anyone who has more top-tier program committee membership at this stage of their career.

Future Potential: In just 5-6 years, Mohit has already established himself as a leader in his research area. He has been consistently publishing high-impact research at flagship venues. He has a thriving research group and has a very impressive funding record. His research is having significant impact both in academia and industry. He is getting invited to positions of prominence, such as program committees of top-tier conferences and research centers. Mohit is a rising star and I have no doubt that he will soar to new heights and become a leader in the wider architecture community.

Comparison with Cohorts: Over the last few decades there have been a few inflection points in computer architecture. I believe right now computer systems are at an inflection point with respect to security. Researchers like Mohit who can understand both security and computer architecture stand to make strong and long lasting impact by defining the primitives for secure architecture of future computing systems. I would rank Mohit's security work as excellent and on par with that of the work of Edward Suh (Cornell), Taesoo Kim (Georgia Tech), and Todd Austin (Michigan).

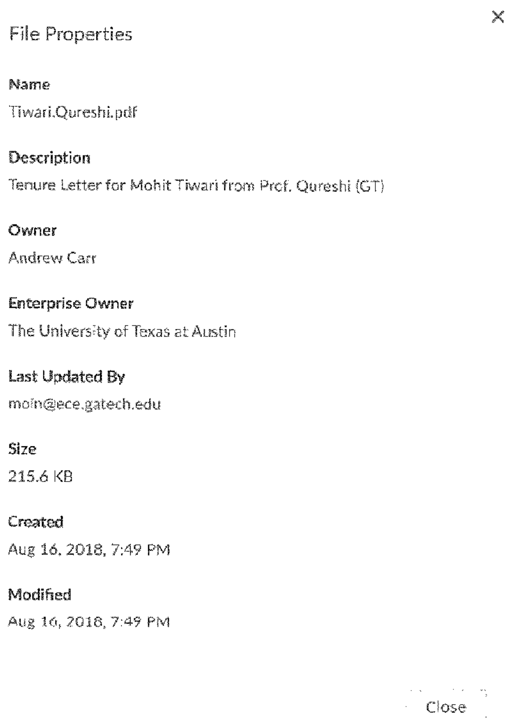
In summary, Mohit's seminal contributions to secure computer systems have had identifiable impact on industry and academic thinking. His research is timely, technologically well grounded, and promises to have influence on the design of secure computing systems of the future. In my opinion, his strong record would clearly earn him tenure at a top-ten university. Mohit has my **unqualified and strongest recommendation** for promotion to Tenured Associate Professor.

Please do not hesitate to contact me if you have any questions.

Sincerely,

Moinuddin K. Qureshi
Professor of Electrical and Computer Engineering,
Georgia Institute of Technology
Email: moin@ece.gatech.edu
Homepage: http://moin.ece.gatech.edu/

Brief Bio of the Letter Writer: Moinuddin Qureshi is a Professor of Electrical and Computer Engineering at the Georgia Institute of Technology. His research interests include computer architecture, memory systems, and quantum computing. Previously, he was a research staff member (2007-2011) at IBM T.J. Watson Research Center, where he developed the caching algorithms for Power-7 processors. He holds more than two-dozen U.S. patents and has 40+ publications in flagship architecture conferences. His publications have received more than 7000 citations, including the unique distinction of having four lead-author papers with more than 500 citations each. He is a member of the Hall of Fame for ISCA, MICRO, and HPCA. He was the Program Chair of MICRO 2015 and Selection Committee Co-Chair of Top Picks 2017. He is a recipient of the Intel Faculty Award (2012), NetApp Faculty Fellowship (2012), and two awards and two honorable mentions at the IEEE MICRO Top-Pick. He received his Ph.D. (2007) and M.S. (2003) from the University of Texas at Austin.



File Properties

Name
Tiwari.Qureshi.pdf

Description
Tenure Letter for Mohit Tiwari from Prof. Qureshi (GT)

Owner
Andrew Carr

Enterprise Owner
The University of Texas at Austin

Last Updated By
moin@ece.gatech.edu

Size
215.6 KB

Created
Aug 16, 2018, 7:49 PM

Modified
Aug 16, 2018, 7:49 PM

BC

UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

Department of Computer Science

201 N. Goodwin
Urbana, IL 61801

Josep Torrellas
Saburo Muroga Professor of Computer Science
Phone: (217)-244-4148
Fax: (217)-265-6582
http://www.cs.uiuc.edu/~torrellas
torrella@illinois.edu

August 9th, 2018

Prof. Ahmed Tewfik
Chair, Department of Electrical and Computer Engineering
School of Electrical and Computer Engineering
University of Texas at Austin

Dear Prof. Tewfik:

This letter is in response to your request to evaluate Prof. Mohit Tiwari, who is being considered for promotion to Associate Professor with tenure at the Department of Electrical and Computer Engineering at the University of Texas at Austin. I know Prof. Tiwari since about 2010, when he was a graduate student at UC Santa Barbara with first-author award papers on security. I have broadly followed his work since then. I have seen him in professional conferences, program committees, and funding meetings. I have read some of his papers and seen him give presentations.

Prof. Tiwari is one of the recognized top leaders of his generation in the area of computer architectures for trustworthy computing. His work is rigorous, impactful, and significant. He has a track record of contributions that result in award papers in computer architecture and computer security. His technical assessments and opinions are typically insightful and balanced. He has significant stature in the academic research community, industry, and federal funding organizations. For these reasons, I would strongly support giving him an Associate Professor position in my department at the University of Illinois.

Since arriving at UT Austin, Prof. Tiwari's research has blossomed. He has produced a large number of publications in the most competitive venues in our field, which include conferences in computer architecture such as HPCA, ASPLOS, and MICRO, and in security such as CCS. These conferences have acceptance rates of 15-20%, and their papers have high visibility among the researchers in the community. Moreover, he has received multiple Award Papers in these conferences, which shows that his work is first class.

I will mention one of his works to illustrate the novelty and potential impact of his work. In his MICRO 2016 paper, he analyzed how to design effective Hardware Malware Detectors (HMD) for mobile systems. HMDs are hardware accelerators based on machine learning classifiers that detect when the software running on the system has the characteristics of malware (e.g., unusual indirect jumps, or repeated calls to websites). To design better HMDs, Prof. Tiwari looked deeply into malware computation, and developed a taxonomy of malware. With his insights, he developed a tool that synthesized malware to specifically find the breaking points of HMDs.

He then developed a new metric for quantifying HMD performance. It is a metric that tells an analyst the root cause behind a malware alert as well as when the HMD fails. Further, Prof. Tiwari used this knowledge and designed better HMDs than prior work. His tool provides insights to analysts to develop better ways to extract program features to train HMDs. Overall, his paper provides a lot of insights and help. His tool was released for public use.

This work was published in the International Symposium on Microarchitecture (MICRO) in 2016. MICRO is one of the very top venues in computer architecture. Papers in such forum have a lot of visibility. The work was well received. Further, I understand that the ideas have been transferred to researchers in Qualcomm, and that this work was the basis of a Qualcomm Faculty Award that Prof. Tiwari received.

Prof. Tiwari will continue to do well. He has sensible and ambitious research plans. They involve a holistic rethink of the field of computer security, and include contributing to cutting-edge topics such as decoy paths and malware detectors. He will continue to publish in visible venues and collaborate with industry.

Prof. Tiwari has visibility that is much higher than his level as Assistant Professor. He has served in the program committees of many top conferences in computer architecture and security. He has been an invited speaker at multiple venues, such as university departments, research organization of companies, and by-invitation workshops. Further, he has been associate editor of an ACM journal and guest editor of a popular IEEE magazine.

The result of all this research work and service is that Prof. Tiwari is highly appreciated in the community. He has received many awards, including the Google, Qualcomm, and Career awards. These are outstanding accomplishments.

Prof. Tiwari has been able to raise an extraordinary amount of research funds. He has received many grants, from the federal government (NSF, DARPA), and industry (Google, SRC, Lockheed-Martin, Huawei, Samsung, Qualcomm, and General Dynamics). This is very unusual, and shows his fine technical and also selling abilities.

He has many PhD students, and already has graduated one. He has a vibrant, active research group. I expect that he will continue to make strong contributions in the years to come.

Overall, Prof. Tiwari is very influential in the area of trustworthy and secure computer architecture thanks to his many contributions. Given that the general area of security is and will become the hottest research area of the next decade, I think his future looks bright. I strongly recommend him for the promotion to Associate Professor.

Sincerely,

JOSEP TORRELLAS

Josep Torrellas
Saburo Muroga Professor of Computer Science
University of Illinois at Urbana-Champaign

SHORT BIO

Josep Torrellas (http://iacoma.cs.uiuc.edu/josep/torrellas.html) is the Saburo Muroga Professor of Computer Science at the University of Illinois at Urbana Champaign (UIUC), where he has been since 1992. He is Fellow of IEEE, ACM, and AAAS. He received the 2015 IEEE Computer Society Technical Achievement Award, and the 2017 UIUC Award for Excellence in Graduate Student Mentoring. He has been the Chair of IEEE Technical Committee on Computer Architecture (TCCA) from 2005 to 2010. Prior to being at Illinois, Torrellas received a PhD from Stanford University.

Torrellas' research interests are computer architectures, technologies and organizations for shared-memory multiprocessors. He has published many works in top conferences and journals and received over 10 Best Paper Awards. He has graduated 36 PhDs, of which 13 are faculty at leading universities, including Cornell, Washington, Georgia Tech, and USC. At Illinois, Torrellas is the Director of the Center for Programmable Extreme Scale Computing, and was the Director of the Illinois-Intel Parallelism Center. He is a member of the Computing Research Association (CRA) Board of Directors, and has served as a Council Member of its Computing Community Consortium (CCC).

From: Torrellas, Josep <torrella@illinois.edu>
Sent: Wednesday, August 15, 2018 10:00 AM
To: Erengil, Jac <jac.erengil@utexas.edu>
Cc: Tewfik, Ahmed H <tewfik@austin.utexas.edu>; Josep Torrellas <torrella@cs.uiuc.edu>
Subject: RE: Promotion Materials, Tiwari

Dear Jac, Ahmed,

Here is the letter. It was an easy one. Best regards

Josep

Josep Torrellas
Saburo Muroga Professor of Computer Science
Computer Science Department
Univ. of Illinois, Urbana-Champaign
Siebel Center for Computer Science
201 N. Goodwin Ave, Urbana, IL 61801

torrella@illinois.edu
Phone: 217-244-4148
Fax: 217-265-6582
http://iacoma.cs.uiuc.edu/~torrellas